NEVADA STATE BOARD OF PHARMACY

POLICY MANUAL 2018

INTRODUCTION

Board members and employees have a duty to carry out and enforce the provisions of Nevada law to protect the health, safety and welfare of the public. *See* NRS 622.080, NRS 639.070(1)(a), NRS 639.213 and NRS 639.2171(1).

General Purpose and Scope

These policies and procedures apply to all Board members and employees. They are not intended to be exhaustive and do not override the specific provisions of law as applied to a particular set of facts. To the extent possible, these policies and procedures are intended to supplement statutes, regulations and executive orders governing the Board, together with the State Administrative Manual and other statewide policies and procedures that apply to all State Executive Branch agencies. If there is a conflict between such other provisions and the provisions of this manual, the other provisions control. In some instances, certain statewide policies and procedures are incorporated by reference in this manual. The Executive Secretary may implement additional policies and procedures not inconsistent with this manual and applicable law.

Employee Input and Improvements

Throughout the Board's history, its employees have been the best source for innovation and improvement of the Board's operations. All employees are encouraged to comment to the Executive Secretary or the General Counsel upon these policies and procedures at any time. These policies and procedures should accurately reflect the actual operations of the Board and lead to greater efficiency in our service to the public.

Review and Changes to the Policies and Procedures

The Board may require changes to these policies and procedures whenever the Board deems necessary. The Executive Secretary and the General Counsel shall review these policies and procedures at least once biennially and make any recommendations for changes to the Board.

No Third-Party Rights

This manual is intended to guide the internal operations of the Board and its staff and is not intended to create any rights, duties, or obligations regarding any person who is a not Board member or employee.

EMPLOYMENT POLICIES

Board employment policies and practices will conform to the requirements of NRS Chapter 281 and Chapter 613.

Employment At Will

Each employee of the Board is employed at will, meaning that the employee may be terminated for any reason or no given reason and with or without any previous disciplinary action or notice. The Executive Secretary serves at the will of the Board. All other employees serve at the will of the Executive Secretary. The Executive Secretary may enlist the assistance of one or more Board members or the entire Board to review applications, interview candidates, or ratify hiring or termination decisions, but the Executive Secretary may also make any employment decisions without the assistance of the Board, as the Executive Secretary deems in his or her discretion to be appropriate or necessary.

Work Hours

An employee is considered full-time if he or she is expected to regularly work 40 or more hours per week. An employee is considered part-time if he or she is expected to regularly work less than 40 hours but more than 24 hours per week. An employee is considered occasional if he or she is expected to regularly work less than 24 hours per week. Occasional employees receive no benefits unless otherwise provided in these policies and procedures. Unless otherwise allowed by the Executive Secretary, every full-time employee is expected to work 40 hours per week.

Compensatory Time

If an employee works 15 or more minutes beyond his or her regular work day or on a weekend or holiday, he or she may record that time as compensatory time. Compensatory time is kept and used in quarter-hour increments. Each employee is responsible to record his or her own compensatory time. The Executive Secretary shall review each employee's total of compensatory time at the end of the calendar year.

An employee may use his or her compensatory time flexibly as long as the use of the compensatory time does not affect pending assignments. An employee needs prior approval from the Executive Secretary or the General Counsel to use compensatory time. Las Vegas employees must also notify the Las Vegas Office Manager of any leave requested before taking any such leave.

An employee may carry forward from one calendar year to the next a maximum amount of compensatory time equal to three times the maximum amount of annual leave he or she is allowed to carry forward from one calendar year to the next. All compensatory time in excess of the allowable maximum will be forfeited on January 1 of each year.

Upon termination of employment, an employee is entitled to be paid for unused compensatory time at his or her regular hourly rate up to the allowable maximum amount, which shall correspondence to the maxim amount for annual leave set forth in the table below. Unlike sick leave and annual leave, compensatory time may not be donated to other employees.

Annual Leave

Annual leave for full-time employees shall accrue and may be accumulated based upon the length of time that the employee has worked for the Board according to the following schedule:

Time Employed	Hrs./Pay Period	Max. Accumulation
5 years or less	3.33 hrs./pay period	160 hours
5 to 10 years	5.00 hrs./pay period	160 hours
10 to 20 years	6.65 hrs./pay period	240 hours
More than 20 years	6.65 hrs./pay period	320 hours

A part-time employee shall accrue and may accumulate annual leave at a rate 75% of that rate that would be allowed to a full-time employee with the same number of years of employment.

An employee should notify the Executive Secretary or the General Counsel and schedule his or her use of annual leave upon the Board's master calendar as soon in advance of the use of the leave as possible (and in the usual case no later than three weeks before the leave) so that the Executive Director and the General Counsel can schedule coverage. Las Vegas employees must also notify the Las Vegas Office Manager of any leave requested before taking any such leave. Reasonable leave requests will be granted unless, in the discretion of the Executive Secretary or the General Counsel, such leave would compromise the efficiency or work of the Board. Employees are encouraged not to seek leave during dates of Board meetings or from September 1 through November 15 of each year. The Executive Secretary may grant leave without prior notice to an employee for unforeseen or unanticipated circumstances of personal misfortune (such as a death of a family member or friend).

At the end of each calendar year, an employee will forfeit any annual leave he or she has accumulated that exceeds the maximum accumulation for that particular employee. An employee will be paid for his accumulated annual leave upon any termination of his or her employment with the Board at his or her most recent hourly rate up to a maximum of the number of annual hours he or she could accumulate.

Annual leave must be taken in half-hour increments. An employee must use compensatory time in excess of 20 hours for any absence from the office before he or she may use annual leave. Employees are encouraged to use their leave throughout the year rather than using it all in the last quarter of the calendar year.

An employee may donate accumulated annual leave to another employee. The terms of the donation, including a determination of whether and how the leave will be repaid, must be made in writing between the two employees and must be approved in writing by the Executive Secretary. A copy of the written agreement must be provided to the Administrative Assistant so that the terms of the agreement can be accommodated by the payroll service. The donor employee will be without recourse if the donee employee terminates his or her employment before he or she has repaid the donated leave.

Sick Leave

Full-time employees accrue sick leave at the rate of 5.0 hours per pay period. Part-time employees accrue sick leave at the rate of 3.75 hours per pay period. There is no limit to the number of hours of sick leave that may be accrued by an employee. An employee whose employment is terminated by reason of retirement or death may receive payment for his or her accrued sick leave at his or her most recent hourly pay based upon the number of years of employment by the Board according to the following schedule:

Time Employed	Maximum Paid
Less than 10 years	None
10 to 15 years	$3,750
15 to 20 years	$6,000
20 to 25 years	$9,000
More than 25 years	$12,000

Whenever possible, an employee should notify the Executive Secretary or the General Counsel (and the Las Vegas Office Manager if the employee is a Las Vegas employee) when he or she intends to use sick leave. Sick leave is only to be used if:

- The employee is unable to perform the duties of his or her position because he or she is sick, injured, or physically incapacitated due to a *bona fide* medical condition.
- The employee is quarantined.
- The employee is receiving medical, psychological, optometric, or dental service or examination.
- A member of the employee's family is sick, injured, physically incapacitated, quarantined, or receiving treatment or examination for a *bona fide* medical condition and the employee is needed to minister, transport, or otherwise assist the family member.

An employee may be asked to provide evidence of the reason given for the use of sick leave by the Executive Secretary or the General Counsel. Misuse of sick leave is a cause for discipline up to and including termination.

Extraordinary Leave

An employee may seek from the Executive Secretary or the General Counsel extraordinary leave under such conditions and for such time as the employee deems needed when:

- The employee is unable to perform his or her duties because of his or her own serious, *bona fide* illness or accident which is life threatening or which will require convalescence exceeding ten working days.
- The employee is unable to perform his or her duties because of the serious, *bona fide* illness or accident which is life threatening or which will require convalescence exceeding ten working days for a member of the employee's family or other person who will rely upon the employee's presence.
- The death of a member of the employee's family or close friend that may require the absence of the employee for more than three working days.
- Any other unforeseen or unfortunate personal circumstance that will require the absence of the employee for more than three working days.

The Executive Secretary or the General Counsel will attempt, as much as possible, to accommodate the employee's request for extraordinary leave. Las Vegas employees must also notify the Las Vegas Office Manager of any leave requested before taking any such leave. An employee will use his or her accrued sick leave (when appropriate), compensatory time, and annual leave for extraordinary leave. If the extraordinary leave will continue beyond all such accrued leave, other employees may donate their accrued leave of any type to assist the employee on extraordinary leave. Throughout the period of extraordinary leave, the employee on extraordinary leave shall call the Executive Secretary or the General Counsel to notify him or her of any significant change of circumstances regarding the leave and when the employee might be able to return to work.

If the extraordinary leave will continue beyond all the employee's accrued leave and the other employees' donations of leave are inadequate to cover the employee's extraordinary leave with pay, the employee and the Executive Secretary shall discuss whether the employee will be allowed to go on leave without pay or whether other arrangements, including termination of the employee's employment, are appropriate.

Miscellaneous Special Leave

Administrative Leave – Administrative leave is leave with pay that is not deducted from the employee's annual or compensatory leave amounts. Administrative leave will be granted an employee under the following circumstances:

- Blood Donation – An employee may take leave with pay for the time necessary to donate blood or blood products (such as platelets) as long as the Executive Secretary or the General Counsel has approved the leave in advance.

- Jury or Witness Duty – An employee will be granted administrative leave for the actual time he or she is required to serve as a juror or as a witness in a court or administrative proceeding other than a hearing or meeting with the Board. Any jury or witness fees must be paid to the Board.

Military Service Leave – An employee who is a member of the National Guard or a Reserve unit of the military will be granted leave for training under the same conditions as would apply to any other request for annual or compensatory leave except that such leave can only be denied by the Executive Secretary if the employee's absence would substantially impair the necessary work of the Board.

Holidays

The Board will observe legal holidays as specified in NRS 236.015, for which all employees will be paid based upon their current salary. If a legal holiday falls on a day within the workweek that is not a regular workday for an employee, that employee shall claim 25% of their regular hours per workweek as compensatory time.

Annual Salary Reviews

Every year before the Board's regularly scheduled meeting in May or June, the Executive Secretary shall review the work of each employee to make a recommendation to the Board regarding potential increases to that employee's salary. The Executive Secretary may recommend a merit increase per employee and may recommend different percentages for each employee depending upon the Executive Secretary's evaluation of the employee's work in the preceding year. At its meeting in May or June, the Board may increase each employee's salary by the percentage increase in the Consumer Price Index for All Urban Consumers (CPI-U) for the West Region for the preceding year plus a merit increase based upon the Executive Secretary's recommendation and the Board's own discretion. Salary increases shall be effective July 1 of each year.

Outside Employment

Before an employee may engage in any employment other than his or her employment with the Board, the employee shall discuss such outside employment with the Executive Secretary or the General Counsel. The Executive Secretary or General Counsel may approve the outside employment as long as it does not constitute a conflict of interest with the operations of the Board, does not create the appearance of impropriety, and does not interfere with the employee's ability to perform his or her functions for the Board.

Travel Expenses

Board members and employees in travel status shall receive reimbursement in accordance with NRS 281.160 and Chapter 0200 of the State Administrative Manual.

Use of Board Equipment and Time

Each employee shall, during his or her hours of duty as an employee and subject to such other laws or regulations as pertain thereto, devote his or her full time, attention and efforts to the business of the Board. Employees may make incidental use of their time and Board property for personal use under the following conditions:

- The use of the property does not interfere with the performance of the employee's duties.
- The cost or value related to the use is nominal.
- The use does not create the appearance of impropriety.

An employee should direct any question regarding whether a particular use of Board property complies with this policy to the Executive Secretary or the General Counsel before the employee makes the personal use of the Board property.

Americans with Disabilities Act

The Board will comply with the Americans with Disabilities Act by following the Employment Provisions Guide for State of Nevada Executive Branch Agencies set forth in Appendix A.

Public Employees' Retirement Program

The Board participates in the Public Employees' Retirement Program (PERS) in accordance with NRS Chapter 286 and will follow the PERS Policies and Procedures for the Retirement System available at https://www.nvpers.org/

Public Employees' Benefits Program

The Board participates in the Public Employees' Benefits Program (PEBP) in accordance with NRS Chapter 287 and will follow the PEBP Policies and Procedures for Employee Health Insurance available at https://pebp.state.nv.us/

Public Employees' Deferred Compensation Program

The Board participates in the Public Employees' Deferred Compensation Program (NDC) in accordance with NRS 287.250-.370 and will follow the NDC Policies and Procedures for the Program available at http://defcomp.nv.gov/

Workers' Compensation Insurance

The Board purchases workers' compensation insurance coverage for employees through a private insurer.

SEXUAL HARASSMENT AND DISCRIMINATION

All Board members and employees are subject to the State of Nevada Executive Branch Sexual Harassment and Discrimination Policy set forth in Appendix B. Each Board member and employee shall sign the acknowledgment therein for retention in the individual's personnel file that he or she has read and understands the Sexual Harassment and Discrimination Policy.

INFORMATION TECHNOLOGY AND SECURITY

All Board members and employees are subject to the State of Nevada Executive Branch Information Security Program Policy set forth in Appendix C. Each Board member and employee shall sign the Acceptable Use Agreement governing the use of Board information technology (IT) resources set forth in Appendix D for retention in the individual's personnel file.

ETHICS IN GOVERNMENT

All Board members and employees are subject to the Nevada Ethics in Government Law, NRS Chapter 281A. Each Board employee shall sign the acknowledgment set forth in Appendix E for retention in the individual's personnel file that he or she has read and understands the Nevada Ethics In Government Manual. Each Board employee shall sign the Policies & Procedures for Screening of Staff to Avoid Conflicts of Interest set forth in Appendix F for retention in the individual's personnel file.

PUBLIC RECORDS

The Board Coordinator is the designated records official for the Board responsible for compliance with the Nevada Public Records Act, NRS Chapter 239, together with NAC Chapter 239, Chapter 0400 and Chapter 2000 of the State Administrative Manual, and State records retention schedules. Board members and employees shall not use their personal electronic devices and personal accounts in the transaction of public business since this generates a public record. The Board shall follow the records retention schedules set forth at

http://nsla.libguides.com/state-records-services/retention-schedules

and the Nevada Public Records Manual available at

http://nsla.libguides.com/ld.php?content_id=34967931.

DUTIES OF THE EXECUTIVE SECRETARY

TEMPORARY LICENSES

The Executive Secretary may only consider a request for a temporary license under NAC 639.200 if the person making the request is a pharmacist and has:

- Filed a fully completed an appropriate application,
- Paid all required fees,
- Nothing in his work or life history that would disqualify him or her or would require an appearance before the Board pursuant to NRS 639.210, and
- Demonstrated a compelling reason for the request.

The Executive Secretary may only consider a request for a temporary license under NAC 639.200 if the requesting party is a pharmacy and has:

- Filed a fully completed and appropriate application,
- Paid all required fees,
- Nothing in its operational history that would disqualify it or would require an appearance before the Board pursuant to NRS 639.210,
- Licenses already with the Board for one or more similar pharmacies, and
- Demonstrated a compelling reason for the request.

If the Executive Secretary grants a temporary license, he shall inform the person making the request of the time after which the license will expire, which time is presumptively 90 days. The Executive Secretary shall report all temporary licenses granted to the Board at each of the Board's meetings.

Responsibility for Employees

The Executive Secretary is responsible for the hiring, discipline, and termination of all employees of the Board. The Executive Secretary has the discretion to assign work among the employees as he or she deems necessary and proper for the efficient and effective function of the Board.

Board members who have questions or concerns regarding the operation of the Board offices or the work of any particular employee should address such questions or concerns to the Executive Secretary. Employees who have questions or concerns regarding their employment or the interpretation of any of these Policies and Procedures should talk with the Executive Secretary regarding their concerns.

Press Relations and Public Speaking

Questions from reporters or the public should be addressed to the Executive Secretary unless another person in the office has been designated by the Executive Secretary to receive such inquiries. Employees should not speak to reporters about anything unless specifically designated to do so by the Executive Secretary. Board members may speak to the press about Board matters, but they are encouraged either to direct the press to the Executive Secretary or to inform the Executive Secretary of the press contact immediately after the press contact. Board members may not speak on behalf of the entire Board unless authorized by the Board to do so. Board members may not discuss with the press anything related to a pending disciplinary matter until the Board has finally ruled in the matter and any judicial review of the matter is concluded.

The Executive Secretary is encouraged to speak to the public regarding issues of interest to the public and the Board related to the practice of pharmacy and the work of the Board. The Executive Secretary may assign public speaking duties to other employees as he or she deems appropriate. The Executive Secretary may seek permission or direction from the Board regarding a given appearance, or from the President if time does not allow for the issue to be raised with the entire Board.

Oversight of Board Finances and Investing of Board Funds

The Executive Secretary has the authority and responsibility to prudently manage the Board's finances. The Executive Secretary may sign contracts on behalf of the Board, may sign negotiable instruments on behalf of the Board, may commit Board funds to investments or other accounts, and may take whatever other action he or she deems necessary to maximize the Board's funds. The Executive Secretary must present a financial report at each meeting of the Board.

The Executive Secretary shall invest the Board's funds as follows:

1. **Cash in Board Checking Accounts**: It is the responsibility of the Executive Secretary to maintain cash balances at levels which enable the Board to meet obligations as they become due. The Executive Secretary may establish a zero-balance checking account where excess cash is invested in a short-term Treasury fund that provides for one-day liquidity; or procure overnight repurchase agreements in order to ensure that funds are not at risk. The Board of Pharmacy will ensure the following:

- The Board members will annually affirm the decision to exceed the FDIC limit of $250,000 when investing in funds approved by statute.
- The limit of $250,000 is only exceeded in institutions with total assets exceeding $10 billion and with a Thompson BankWatch or equivalent issuer rating of B/C or better.
- Institutions are scrutinized annually to ensure that the high ratings are maintained.

2. **Acceptable investments for funds not required for satisfying current obligations.** The Executive Secretary shall determine the investments based on its cash flow needs and safety and liquidity of investment. The Executive Secretary may invest Board funds that are not needed for current obligations only in the following:

- Savings accounts protected by U.S. Government guarantees, interest bearing demand accounts, time or certificates of deposits in banks and savings and loan institutions physically located within Nevada. The Board of Pharmacy will ensure the following:
  - The Board of Pharmacy members will annually affirm the decision to exceed the FDIC limit of $250,000.
  - The limit of $250,000 is only exceeded in institutions with total assets exceeding $10 billion and with a Thompson BankWatch or equivalent issuer rating of B/C or better.
  - Institutions are scrutinized annually to ensure that the high ratings are maintained.
- U.S. Treasury bills, notes and bonds. Securities issued by U.S. Government agencies such as: Federal Farm Credits, Federal National Mortgage Association and Federal Home Loan Association. These securities may not have maturities greater than 10 years. Average maturities may not exceed five years. Board will not invest in securities of more than 24 months.

3. **There shall be no investment of Board funds in**:

- State, local, or corporate notes and bonds.
- Equities (common and preferred stocks or long-term investments).
- Short-term Treasury Mutual Funds.
- Money Market Mutual Funds.

Operating Reserves

The Executive Secretary shall ensure compliance with the Board's reserve policy set forth in Appendix G.

Contract Approval

The Executive Secretary shall ensure compliance with the requirements of NRS Chapter 333, NAC Chapter 333, and Chapter 0300 of the State Administrative Manual for all contracts.

Financial Reporting

The Executive Secretary shall ensure compliance with the financial reporting requirements of NRS 218G.400.

DUTIES OF THE DEPUTY EXECUTIVE SECRETARY

The Deputy Executive Secretary shall be a licensed pharmacist in this State and shall perform those duties assigned by the Executive Secretary, which may include the authority to act on behalf of the Executive Secretary when the Executive Secretary is absent from the Board offices or otherwise unavailable, including, without limitation, the authority to sign accusations on behalf of the Executive Secretary pursuant to NRS 639.241(2). The Deputy Executive Secretary may have signature authority on the Board's bank, investment, and credit accounts.

DUTIES OF THE LAS VEGAS OFFICE MANAGER

The Las Vegas Office Manager shall have the following responsibilities, duties, and obligations for the Board:

- Day-to-day operations and activities of the Las Vegas office
- Disseminating information to the Executive Secretary or the General Counsel regarding situations, news articles, and any other information pertinent to or that would affect the Board
- Assuring that the Las Vegas office operates similarly to the Reno office
- Overseeing the day-to-day activities of the Las Vegas staff in order to coordinate with the Reno office regarding investigation and inspection assignments
- Carrying out the policies, procedures, and directives of the Executive Secretary and the General Counsel
- Controlling the use of the Board's credit card to assure it is used only for allowable purchases, including consulting with the Reno office regarding such use of the Board's credit card
- Assuring that the Las Vegas staff have the necessary support and assistance to carry out its functions
- Assuring that the Las Vegas staff cares for its assigned equipment and cars, including surplusing or replacing equipment when needed
- Reporting to the Executive Secretary and General Counsel regarding the performance of Las Vegas staff

DUTIES OF THE GENERAL COUNSEL

Legal Duties

The General Counsel shall have the following legal responsibilities and obligations for the Board, subject to the requirements and restrictions of the Nevada Rules of Professional Conduct:

- Taking any action on behalf of the Board deemed necessary to protect the State's legal interests until such time as the Board may adequately consider the matter
- Providing day-to-day legal advice to Board members and employees on matters over which the Board has supervision, control, jurisdiction or advisory power
- Drafting and reviewing legal papers and correspondence
- Preparing and prosecuting disciplinary actions
- Representing the Board in all legal proceedings
- Representing the Board before legislative committees
- Drafting regulations and bill drafts
- Advising the Board at its meetings except when the General Counsel is prosecuting disciplinary cases, in which case the Board is advised by a representative of the Attorney General's Office
- Responding to simple inquiries from the public, licensees, or applicants for licensure on Nevada's pharmacy laws, which shall not constitute legal advice

General Counsel Authority to Act

The General Counsel is hereby authorized and directed to take any action on behalf of the Board deemed necessary to protect the State's legal interests until such time as the Board may adequately consider the matter. This may include filing a response to a petition for judicial review of a final decision of the Board in a contested case. This may also include filing a protective notice of appeal from an adverse ruling or judgment whenever the Board, for any reason, is unable to take action on an appeal during the prescribed statutory period for taking an appeal. Under such circumstances, the Board will thereafter act, in the normal course of business, to ratify, or direct dismissal, of the appeal.

Administrative Duties

The General Counsel also has all the responsibilities, duties, and authority of the Executive Secretary when the Executive Secretary or Deputy Executive Secretary are both absent from the Board offices or otherwise unavailable. The General Counsel may have signature authority on the Board's bank, investment, and credit accounts. The General Counsel will also perform such duties as are assigned from time-to-time by the Executive Secretary.

BOARD VEHICLES

Investigators and Inspectors will be provided vehicles for their use whenever they are on Board business. Other Board staff and Board members are authorized to use Board vehicles for Board functions. The use of Board vehicles must comply with Chapter 1300 of the State Administrative Manual and the following:

- **Use a Board vehicle when on Board business.** If an employee will be conducting Board business on a given day or portion of a day within 15 minutes of his or her home, the employee may use his or her personal vehicle for his or her own convenience for that day or portion of a day, but such use will not be reimbursed for mileage. If an employee must use his or her personal vehicle because a Board vehicle is unavailable, the employee will be reimbursed at the standard mileage reimbursement rate authorized by the Governor's Finance Office Budget Division.
- **Leave Board vehicles at the Board office when no longer on Board business.** Occasionally an Investigator or Inspector may be asked by a Board member, the Executive Secretary, or the General Counsel to leave a Board car somewhere else, such as at a hotel or airport, in which case the Inspector or Investigator should do so.
- **Pursuant to NRS 204.080 private use of a Board vehicle is prohibited.**
- **Maintain Board vehicles.** Each Inspector or Investigator is responsible to make sure that his or her Board vehicle receives regular maintenance including oil changes (every 3,500 miles), tire rotations, tune-ups, and washings as needed, with prior authorization from the Executive Secretary. The Board will not reimburse inappropriate or unapproved expenses such as running out of fuel, running down the battery, charges for lost keys, parking citations, or traffic tickets or other moving violations.
- **Report traffic tickets.** Any employee or Board member who drives a Board-provided car must report to the Executive Secretary immediately any traffic ticket. Violation of this policy by receiving excessive traffic tickets, by receiving traffic tickets for driving behavior that endangers the employee or the public, or by failing to report a traffic ticket to the Executive Secretary immediately may result in discipline, including termination of employment.
- **Operating a Board vehicle under the influence of alcohol or drugs is prohibited.** Violation of this policy could result in discipline, including termination, regardless of whether the employee was arrested or charged with such conduct.
- **Damage to the car that did not result from an accident must be reported to the Executive Secretary or the General Counsel immediately.**

Accident Procedure

Any Board member or employee who has an accident involving a Board vehicle must follow the provisions of Chapter 2900 of the State Administrative Manual and the following procedure:

- **Remain on the scene and immediately notify the appropriate law enforcement agency, give the exact location and advise them if there are any injuries.**
- **Notify the Executive Secretary or the General Counsel immediately.** The employee must notify the Executive Secretary or the General Counsel of the extent of injuries of all parties involved and the extent of the property damage to the extent this information is available.
- **Obtain the name, address, and car license numbers of other parties and the names and addresses of witnesses, and document the accident with photos or video to the extent feasible.**
- **Complete law enforcement and risk management accident reports. DO NOT SIGN OR MAKE A STATEMENT AS TO RESPONSIBILITY.**
- **The State Accident Report (Form No. RSK-001) MUST be submitted within two working days to the Executive Secretary.** The Executive Secretary must submit the form immediately upon receipt to the Department of Administration Risk Management Division.

FINANCIAL ADMINISTRATION

Internal Accounting and Administrative Control

The Executive Secretary shall implement a system of internal accounting and administrative control for the Board subject to the following limitations:

- Incoming mail shall be logged by Board staff other than the Director of Finance or the Licensing Specialist.
- The Licensing Specialist shall review all checks and money orders for payment of licensing fees and make all deposits.
- The Board shall not accept cash payments.
- Only the Executive Secretary, Deputy Executive Secretary and General Counsel may have signature authority on the Board's bank, investment, and credit accounts.

Grants Management

The Board shall comply with the applicable Grants Management Common Rule for any federal grant funds, including, without limitation, 2 CFR Part 200.

LEGAL AND ADMINISTRATIVE ACTIONS

Defense and Indemnification

Generally, the State will defend and indemnify Board members and employees for actions taken in good faith within the scope of their statutory duties. The Board pays premiums into the State Tort Claims Fund. However, Board members and employees must comply with the requirements of NRS Chapter 41 and Chapter 2900 of the State Administrative Manual for defense and indemnification.

Service of Process

Board members and employees shall immediately notify the General Counsel and the Office of the Nevada Attorney General whenever served with a complaint in federal or state court, or a petition for judicial review, or if otherwise presented with legal documents, since service must be effected in strict compliance with FRCP 4(j)(2), NRS 41.031(2) or NRS 233B.130(2), which includes service upon the Office of the Nevada Attorney General.

Documentation of Attorney's Fees and Costs

The Board may recover reasonable attorney's fees and costs that are incurred as part of its investigative, administrative and disciplinary proceedings pursuant to NRS 622.400. In any matter that results in disciplinary action, whether by stipulated settlement or by Board order following a hearing, the Board may order reimbursement for expenses necessarily incurred in protecting the public. This may include, without limitation, time and travel costs incurred by Investigators in the investigation of the matter, the General Counsel in the prosecution of the matter, the Board Coordinator in providing legal support, Board members in hearing the matter, witnesses and expert witness fees, and the Office of the Nevada Attorney General in serving as Board counsel.

The Board may also recover reasonable attorney's fees and costs that are incurred as a prevailing party in judicial actions related to the Board's enforcement authority pursuant to NRS 622.410.

The Board must document that attorney's fees and costs are both reasonable and actual; therefore, Investigators, the General Counsel and the Board Coordinator will document their time on the investigation and prosecution of any disciplinary matter, or on any litigation related to the Board's enforcement authority, using a timekeeping system approved by the General Counsel.

COMPLAINT INVESTIGATION PROCEDURES

The following procedures for the investigation of complaints should be followed by Investigators in the usual course. Deviation from the procedures may occur from time to time as situations and circumstances require, but such deviations should be approved in advance by the Executive Secretary whenever practicable.

1. **The Executive Director and General Counsel will conduct an initial review of all complaints submitted.** The review will include an initial screening consistent with the Policies & Procedures for Screening of Staff to Avoid Conflicts of Interest set forth in Appendix F. The review will also include a determination of whether the complaint is against licensee(s), whether the matter is within the Board's jurisdiction or the jurisdiction of another board, and whether the complaint states a claim. If the complaint is within the Board's jurisdiction and warrants investigation, the matter will be referred to the Board Coordinator. If the complaint appears within the jurisdiction of another board, it will be referred to the appropriate board. If the complaint does not warrant an investigation and/or fails to state a claim, the General Counsel will respond in writing as necessary.
2. **Board Coordinator logs in complaints, assigns them a number, and routes them to the appropriate Investigator.** The Board Coordinator should process the complaint within one working day of receipt.
3. **The Investigator contacts the complainant within two working days after receiving the complaint.** Unless the Investigator feels that early contact with the complainant would impair the investigation, the Investigator should make initial contact with the complainant as soon as possible.
4. **The complaint is investigated in a timely manner.** The Board staff has broad legal authority to access and inspect premises and records. Investigators should request that the Executive Secretary issue subpoenas for the production of witnesses, documents or papers to the extent necessary. As questions or tactical decisions arise, Investigators should consult the Executive Secretary or General Counsel.
5. **The Investigator submits a report to the Board Coordinator.** Investigators should prepare a detailed narrative report on the standard form. The report should attach copies or references to the evidence collected in the investigation, including written or recorded statements of witnesses. The factual assertions that form the basis for the findings and conclusions in the report and any allegations of violations of law should not be based solely on uncorroborated hearsay but must be supported by direct evidence. The report should also document the time expended by the Investigator on the case.
6. **The Investigative Committee will review the report and determine how to proceed.** The Investigative Committee will be comprised of the Executive Secretary, the General Counsel, the Board Coordinator, and, if required, the Investigator(s) involved in the investigation.

INSPECTION PROCEDURES

The Board staff has broad legal authority to access and inspect premises and records. The following inspection procedures should be followed by Inspectors in the usual course. Deviation from the procedures may occur from time to time as situations and circumstances require, but such deviations should be approved in advance by the Executive Secretary whenever practicable. Following should be the usual steps in the inspection process:

1. **The Administrative Assistant notifies the pharmacies and facilities to be inspected in the first week of the month preceding the month in which the inspection will occur.** The notification will consist of a form letter, a pre-inspection form, and a workplace assessment tool with instructions that the pharmacy would need to have the forms completed and all materials available for a random inspection one month later. (For example, the materials would be provided in the first week of January for facilities that would be inspected in February.)
2. **The Administrative Assistant notifies the Inspector of the pharmacies and facilities to be inspected one week before the inspections will occur.** On a monthly basis, the Administrative Assistant will schedule pharmacies and facilities to be inspected based upon locale and will notify the Inspectors of their upcoming inspections one week before the actual inspections are to occur. The Administrative Assistant shall also notify the General Counsel and the Las Vegas Office Manager of the weekly assignments so that questions of rescheduling or efficiency can be addressed to them.
3. **The Inspector conducts the assigned inspections unannounced.** The Inspector will visit the assigned inspections in such order as he or she deems efficient, as long as the weekly assignments are completed. The managing pharmacist is not required to be present at an inspection, nor are appointments to be made. Inspectors should minimize disruption of the pharmacy's operations by doing inspections as unobtrusively as possible. Inspectors should request the production of any records necessary to an inspection and must note all deficiencies to be addressed and corrected. Inspectors should shall immediately notify the General Counsel if the issuance of an administrative warrant is necessary.
4. **The Inspector sends the completed inspection forms to the Administrative Assistant.** The Administrative Assistant will log in the date of completion of all inspection forms.
5. **The Administrative Assistant responds appropriately to all notes on the inspection forms.** If the Inspector has noted deficiencies, the Administrative Assistant will prepare a letter for the Executive Secretary's signature to the pharmacy or facility informing the pharmacy or facility of the time within which the deficiency must be addressed and corrected. The Administrative Assistant will also log and schedule the follow-up visit (when appropriate) by putting the follow-up visit on the appropriate schedule for the Inspector.

6. **The Administrative Assistant will follow-up on deficiencies.** Where a letter has been sent regarding deficiencies and the deficiencies have not been timely addressed and corrected, the Administrative Assistant will notify the Board Coordinator of the failure to remedy the deficiencies so that the Board Coordinator can open a complaint matter against the pharmacy or facility.
7. **The Administrative Assistant will prepare reports.** The Administrative Assistant will enter the workplace assessment tool data into the Board's computer system within five business days of receipt of the reports from the Inspector. The Administrative Assistant will prepare and provide to the General Counsel at least quarterly a status report of the inspections completed by each Investigator.

ELECTION OF BOARD OFFICERS

NRS 639.040(1) requires the Board to elect a President and a Treasurer from among its members. The election of Board officers will be conducted under the following procedure:

1. The Board will hold an election for the offices of President and Treasurer at the regularly-scheduled meeting in June of even-numbered years.
2. The term of office will commence at the next Board meeting for a period of two years.
3. The outcome of the election will be determined by majority vote.
4. There will be no term limits.
5. In the event of the termination of an officer's tenure on the Board, an election will be held at the next regularly-scheduled Board meeting to fill the vacancy.

THE AMERICANS WITH DISABILITIES ACT (ADA) & THE ADA AMENDMENTS ACT (ADAAA)

Employment Provisions Guide for State of Nevada Executive Branch Agencies

January 2018

INTRODUCTION

This guide discusses the application of the employment provisions of the Americans with Disabilities Act (ADA) of 1990. The ADA is a federal antidiscrimination statute designed to remove barriers, which prevent individuals with disabilities who are qualified from enjoying the same employment opportunities, services and privileges available to persons without disabilities. The ADA Amendments Act (ADAAA), effective January 1, 2009, was adopted by Congress with the intention of restoring the original intent of the ADA by providing a clear and comprehensive national mandate for the elimination of discrimination.[1] The ADAAA overturns several United States Supreme Court decisions that had limited coverage under the ADA.

Like the Civil Rights Act of 1964 that prohibits discrimination on the basis of race, color, religion, national origin, and sex, the ADA seeks to ensure access to employment opportunities based on merit. It does not guarantee equal results, establish quotas, or require preferences favoring individuals with disabilities over those without disabilities. However, while the Civil Rights Act of 1964 prohibits any consideration of personal characteristics such as race or national origin, the ADA takes a different approach. When an individual's disability creates a barrier to employment opportunities, services or privileges, the ADA requires an employer to consider whether reasonable accommodation could remove the barrier.

While the ADA focuses on eradicating barriers, it does not relieve an individual with a disability from the obligation to perform the essential functions of a position. To the contrary, the ADA is intended to enable an individual with a disability who is qualified to access the privileges and services offered and to compete in the workplace based on the same performance standards and requirements that agencies expect of individuals who are not disabled. However, where an individual's functional limitation(s) impedes job performance, an employer must take steps to reasonably accommodate, and thus help overcome the particular impediment(s), unless to do so would impose an undue hardship.

The process of identifying whether, and to what extent, a reasonable accommodation is required should be flexible, made on a case-by-case basis and requires participation by both the employer and individual. No specific form of accommodation is guaranteed to all individuals with a particular disability; however, the accommodation process must be consistent and non-discriminatory. An accommodation must be tailored to match the needs of the individual with a disability and the needs of the individual’s position.

State government is a covered entity for the purposes of the ADA and must comply with the non-discrimination provisions of the ADA.

This guide is not a substitute for legal advice and is subject to change without notice. If you need specific information regarding the ADA, consult your human resources staff, your agency's

attorney, federal and State enforcement and technical assistance agencies or the Division of Human Resource Management (see Resources & References).

What is a disability as defined by the ADA (ADAAA)?

- A physical or mental impairment which substantially limits one or more major life activities;
- A record of an impairment; or
- Being regarded as having an impairment.

WHAT IS A DISABILITY?

It is important to remember that the definition of disability, as defined by the ADA, is legal and not medical. If an individual is deemed "disabled" under a different law (e.g., Social Security Act) it does not mean that the individual automatically meets the definition of disability under the ADA/ADAAA.

Also an individual may be covered by more than one of the definitions of disability.

PHYSICAL OR MENTAL IMPAIRMENT WHICH SUBSTANTIALLY LIMITS ONE OR MORE MAJOR LIFE ACTIVITIES

PHYSICAL OR MENTAL IMPAIRMENT

The ADAAA specifically states that the definition of disability should be interpreted broadly and that determining whether "an individual's impairment is a disability under the ADA should not demand extensive analysis".[1]

A physical impairment is defined by the Equal Employment Opportunity Commission (EEOC) as any physiological disorder, or condition, cosmetic disfigurement, or anatomical loss affecting one or more body systems such as neurological, musculoskeletal, special sense organs, respiratory (including speech organs), cardiovascular, reproductive, digestive, genitourinary, immune, circulatory, hemic and lymphatic, skin, and endocrine. A mental impairment is defined by the EEOC as any mental or psychological disorder, such as an intellectual disability, organic brain syndrome, emotional or mental illness, and specific learning disabilities.[2]

The definition of the term "impairment" does not include physical characteristics such as eye color, hair color, left handedness, or height, weight or muscle tone that are within "normal" range and are not the result of a physiological disorder. Similarly, the definition does not include common personality traits such as poor judgment or a quick temper where they are not symptoms of a mental or psychological disorder. Environmental, cultural, or economic disadvantages such as poverty, lack of education or a prison record

are not impairments. Advanced age, in and of itself, is also not an impairment.

MAJOR LIFE ACTIVITIES

What is a major life activity? A major life activity is a basic activity that most people in the general population can perform with little or no difficulty.

Major life activities include, but are not limited to:

- Caring for oneself
- Performing manual tasks
- Seeing
- Hearing
- Eating
- Sleeping
- Walking
- Standing
- Sitting
- Reaching
- Lifting
- Bending
- Speaking
- Breathing
- Learning
- Reading
- Concentrating
- Thinking
- Communicating
- Interacting with others

- Working
- Operation of a major bodily function

MAJOR BODILY FUNCTIONS

Major bodily functions are included as major life activities and may include, but are not limited to:

- Functions of the immune system
- Special sense organs and skin
- Normal cell growth
- Digestive
- Genitourinary
- Bowel
- Bladder
- Neurological
- Brain
- Respiratory
- Circulatory
- Cardiovascular
- Endocrine
- Hemic
- Lymphatic
- Musculosketal
- Reproductive

SUBSTANTIALLY LIMITS

A common sense assessment based on comparing an individual's ability to perform a specific major life activity with most people in the general population is used to determination whether an impairment "substantially limits". The ADAAA indicated that a limitation need not

"significantly" or "severely" restrict a major life activity to meet the standard of "substantially limits".[1]

The EEOC regulations provide rules to use when determining whether an impairment is substantially limiting.

1. The term "substantially limits" should be construed broadly in favor of expansive coverage, to the maximum extent permitted by the terms of the ADA.
2. An impairment is a disability if it substantially limits the ability of the individual to perform a major life activity as compared to most people in the general population.
3. Determination of whether an impairment substantially limits a major life activity should not demand extensive analysis.
4. The determination of whether an impairment substantially limits a major life activity requires an individualized assessment.
5. The comparison of a major life activity to the performance of the same major life activity by most people in the general population will not require scientific, medical or statistical analysis.
6. The determination of whether an impairment substantially limits a major life activity shall be made without regard to ameliorative (improving) effects of mitigating measures.
7. An impairment that is episodic or in remission is a disability if it would substantially limit a major life activity when active.
8. An impairment that substantially limits one major life activity need not substantially limit other major life activities in order to be considered a substantially limiting impairment.
9. The effects of an impairment lasting or expected to last fewer than six months can be substantially limiting.[2]

MITIGATING MEASURES

The positive effects of mitigating or compensating measures cannot be considered when determining whether an individual meets the definition of disability. However, the negative effects of mitigating factors may be considered.

Mitigating measures, may include, but are not limited to:

- Medications
- Medical supplies

- Equipment or appliances
- Low-vision devices (which do not include ordinary eyeglasses or contact lens)
- Prosthetics including limbs and devices
- Hearing aids and cochlear implants or other implantable hearing devices
- Mobility devices
- Oxygen therapy equipment and supplies
- Use of assistive technology
- Reasonable accommodations or auxiliary aids or services
- Learned behavioral or adaptive neurological modifications
- Surgical intervention, except where it has permanently eliminated the impairment

The one mitigating factor that may be considered in determining whether an individual is disabled is the use of "ordinary eyeglasses or contact lenses" that are intended to fully correct the individual's visual acuity or refractive error.[1]

PREDICTABLE ASSESSMENTS

The EEOC regulations give examples of impairments that will, in virtually all cases, result in a determination of substantial limitation of a major life activity.[2] For this reason, the individualized assessment of the limitations on the individual should be simple and straightforward. The examples are:

- Deafness
- Blindness
- Intellectual disability
- Partially or completely missing limbs
- Mobility impairments requiring the use of a wheelchair
- Autism
- Cancer
- Cerebral palsy
- Diabetes

- Epilepsy
- HIV/AIDS
- Multiple sclerosis (MS)
- Muscular dystrophy
- Major depression
- Bipolar disorder
- Post-traumatic stress disorder (PTSD)
- Obsessive compulsive disorder
- Schizophrenia

RECORD OF AN IMPAIRMENT

An individual would have a record of a disability if the individual had a history of, or was misclassified previously as having, an impairment that substantially limits one or more major life activity.

For example, a cancer survivor would be an individual with a record of an impairment. Or an individual, who was incorrectly diagnosed with bipolar disorder due to a reaction to medication, also has a record of an impairment even though the individual did not actually have the disorder.

"REGARDED AS" HAVING AN IMPAIRMENT

An individual is "regarded as" having a disability if:

1. Subjected to an employment action prohibited under the ADA; and

2. The action was taken because of an actual or perceived impairment regardless of whether the impairment is, or is perceived to be, substantially limiting a major life activity.

Regarding an individual as disabled could include taking a prohibited action based on symptoms of an impairment or the use of mitigating measures.

An employee who is only "regarded as" having a disability is not entitled to accommodation.

TRANSITORY AND MINOR

An individual is not "regarded as" having an impairment, if the impairment is both transitory and minor. A transitory impairment is an impairment with an actual or expected duration of 6 months or less.

ALCOHOL

Alcoholism can, in some circumstances, meet the standard of a covered disability. However, an employer does not have to allow either consumption of alcohol on duty or an employee being under the influence while working.

CONTROLLED SUBSTANCES

Individuals who currently use controlled substances illegally are not individuals with disabilities protected under the Act. This includes individuals who use prescription drugs illegally as well as those who use illegal controlled substances. However, individuals who have been rehabilitated and do not currently use controlled substances illegally may be protected under the ADA.

EXCLUSIONS

Pregnancy in of itself is not a disability as defined by the ADA.

The following conditions are also excluded from the definition of disability under the ADA:

- Pedophilia
- Exhibitionism
- Voyeurism
- Other sexual behavior disorders
- Compulsive gambling
- Kleptomania
- Pyromania
- Psychoactive substance use disorders resulting from current illegal use of controlled substances

IMPACT ON EMPLOYMENT PRACTICES

The ADA/ADAAA prohibits discrimination based on disability in regards to:

- Recruitment, advertising, job application;
- Hiring, promotion, demotion, transfer, layoff, termination, return from layoff, rehire;
- Discipline;
- Compensation;
- Job assignments, job classifications, organizational structures, position descriptions, seniority;
- Leave;
- Benefits;
- Training;
- Sponsored activities; or
- Any other term, condition or privilege of employment.

DISCRIMINATION

Discrimination under the ADA includes limiting, segregating, classifying, harassing, retaliating, denying or otherwise making an employment decision based on an individual's disability. Discrimination is also prohibited under an agency's contracts with any other entity (i.e. benefits, training).

The ADAAA does not protect an individual who is denied an employment opportunity or a reasonable accommodation because he or she does not have a disability.

ASSOCIATION PROVISION

Discrimination can also be based on a relationship with someone with a disability. The word relationship, as used in this context, is not limited to family relationships; it can include association with an individual with a disability. The EEOC states that the intent of the provision is "to prevent employers from taking adverse actions based on unfounded stereotypes and assumptions about individuals who associate with people who have disabilities."[5] Refusing to hire an individual with a spouse with a disability based on the assumption that he or she would have to frequently be absent from work to take care of his or her spouse, would be an example of discrimination based on association with an individual with a disability. Accommodation does not have to be provided

to an individual without a disability due to that individual's association with someone with a disability.

ESSENTIAL FUNCTION

Essential functions are so necessary to the position that an individual cannot do the job without being able to perform them.

MARGINAL FUNCTIONS

Marginal functions can be described as peripheral, minimal, extra, borderline, incidental and/or nonessential. Marginal functions can be reassigned to another individual without compromising the core of the position's duties.

ESSENTIAL FUNCTIONS DEVELOPMENT

It is important to establish or re-evaluate the essential functions of a position before taking an employment action such as recruiting, hiring or promoting. Also, the essential functions of a position should be reviewed and revised as needed when the work performance standards are updated.

To establish the essential functions of a position, the position must be clearly defined and its component tasks and requirements analyzed to determine the physical and mental demands these tasks place on the employee and the environmental conditions in which the position is performed.

The factors to be considered in determining whether a function is essential are, as outlined in federal regulation are:

- Whether the position exists to perform the function;
- The number of other employees available among whom the performance of that function can be distributed;
- The degree of expertise or skill required to perform the function; and
- Whether an employee is currently performing or has performed the function;

What is an essential function?

Essential functions are so necessary to the position that an individual cannot do the job without being able to perform them.

- The consequences of not requiring the incumbent to perform the function;
- The amount of time spent performing the function.

When identifying essential functions, it is important not to confuse method with function. For example, it would not be correct to say that an employee has to “drive to meetings” when the actual task is to “attend meetings”. Do not make assumptions about what the position does, such as relying on job titles or traditional roles.

Keep in mind that functions that are performed infrequently or little time is spent on can also be considered essential. The deciding factor may be the consequence of not performing the function. For example, a firefighter may only occasionally have to carry a person from a burning building but it is still an essential function.

The agency’s judgment is a factor in determining which functions are essential.

The Essential Functions Position Analysis form (ADA-1) was developed to assist in identifying which functions are essential. Class specification, work performance standards, Position Questionnaire (NPD-19), the employee that currently is in the position and the employee's supervisor are excellent resources in determining what functions are actually performed and the factors that determine whether they are essential or marginal.

The Physical and Cognitive Characteristics Inventory form (ADA-2) may also be used in developing the essential functions for a position.

The essential functions of a position are documented on the Position Functions form (ADA-3).

MEDICAL INQUIRIES

The rules on medical inquiries/examinations apply to all employees, not just those with a disability.

The EEOC has stated that medical examinations include, but are not limited to:

- "vision tests conducted and analyzed by an ophthalmologist or optometrist;
- blood, urine, and breath analyses to check for alcohol use;
- blood, urine, saliva, and hair analyses to detect disease or genetic markers (e.g., for conditions such as sickle cell trait, breast cancer, Huntington's disease);
- blood pressure screening and cholesterol testing;
- nerve conduction tests (i.e., tests that screen for possible nerve damage and susceptibility to injury, such as carpal tunnel syndrome);
- range-of-motion tests that measure muscle strength and motor function;

- pulmonary function tests (i.e., tests that measure the capacity of the lungs to hold air and to move air in and out);
- psychological tests that are designed to identify a mental disorder or impairment; and,
- diagnostic procedures such as x-rays, computerized axial tomography (CAT) scans, and magnetic resonance imaging (MRI)."[3]

Tests for illegal use of drugs, physical agility, the ability to read and evaluate objects, psychological tests that measure personality traits such as honesty, preferences and habits and polygraph examinations are generally not considered medical examinations under the ADA and not subject to the ADA restrictions on such examinations.[3]

PRE-OFFER

An employer may not inquire as to whether an individual has a disability or conduct a medical inquiry/examination prior to a conditional offer of employment. Nor can an employer inquire at the pre-offer stage about an applicant's workers' compensation history. Agencies may ask questions that relate to the applicant's ability to perform job-related functions. However, these questions should not be phrased in terms of disability. If there is a reasonable belief that a candidate will not be able to perform a job function because of a known disability, a candidate may be asked to describe or to demonstrate how, with or without reasonable accommodation, the candidate would perform a job-related function(s) during an interview. However, a candidate may not be asked for information regarding the possible disability nor should the request for a description or demonstration of how the candidate would perform a job function(s) be made more than once.

A test that is not a medical examination would not be subject to the prohibition against pre-employment medical examinations if given to all similarly situated applicants or employees, regardless of disability. However, if such a test screens out or tends to screen out an individual with a disability or a class of such individuals because of disabling condition(s), the State or agency must be prepared to show that the test is job-related and consistent with business necessity and also that the test or the essential function cannot be performed with a reasonable accommodation.

POST-OFFER

An employer may condition a job offer on the satisfactory result of a pre-employment and post-offer medical examination or inquiry if this is required of all candidates in the same position or class; however, the examination or inquiry must comply with GINA.

If an individual is not hired because a pre-employment and post-offer medical examination or inquiry reveals a disability, the reason(s) for not hiring must be job-related and consistent with business necessity. The employer also must show that no reasonable accommodation was

available that would enable this individual to perform the essential job functions or that the accommodation that would allow the individual to perform the essential job functions would impose an undue hardship.

A pre-employment, post-offer medical examination may also disqualify an individual who would pose a direct threat to health or safety. Such a disqualification is job-related and consistent with business necessity. However, again the employer also must show that no reasonable accommodation was available that would lower the threat to an acceptable level.

A pre-employment and post-offer medical examination may not disqualify an individual with an impairment who is currently able to perform the essential job functions because of speculation that the impairment may cause a risk of future disability.

AFTER EMPLOYMENT

Medical questions or evaluations after employment must be job related and consistent with business necessity. Generally an evaluation meets that standard when the agency "has a reasonable belief, based on objective evidence, that: (1) an employee's ability to perform essential job functions will be impaired by a medical condition; or (2) an employee will pose a direct threat due to a medical condition."[3]

Agencies may also additionally conduct post employment medical examinations for the following reasons:

- The examinations are required by federal law or regulation; or
- When the examination is voluntary (neither requiring participation nor penalizing for not participating[3]) and a part of an employee health program.

BACKGROUND AND REFERENCE CHECKS

The rules regarding what medical information may be requested pre-offer, post-offer and after employment also apply to background and reference checks. In general, the EEOC takes the perspective that a job offer is real only if all relevant non-medical information (e.g., background and reference checks) which reasonably could be obtained are analyzed prior to giving the offer. However, the EEOC has recognized that there are times when an employer cannot reasonably obtain and evaluate all non-medical information at the pre-offer stage.[13]

RECRUITMENT

In general, the ADA does not require employers to take affirmative action in employing people with disabilities (i.e., agencies are not required by the ADA to recruit, hire and promote individuals with disabilities as part of a mandate to make their work force more diverse). Rather, the ADA

requires agencies to modify their hiring processes and employment practices so that discrimination does not occur when a person with a disability applies or is hired.

However, the ADA does not invalidate Section 503 of the Rehabilitation Act, which requires federal contractors and subcontractors with contracts and subcontracts of $10,000 or more per year to take affirmative action in hiring and promoting individuals with disabilities.

It is generally recommended to base a job posting/notice/advertisement on the essential functions.

Accommodation may be requested in the application and interview processes.

INTERVIEWING

The prohibition on pre-offer medical inquiries also applies to questions asked during interviews. Locations for interviews should be accessible and an applicant is entitled to accommodation for the interview.

NAC 284.441 requires the appointing authority to provide a description of the essential functions of the position to each applicant who is being considered for a position. The information must be provided in a timely manner to allow an applicant with a disability to determine his or her need for reasonable accommodation.

SELECTION PROCESS

It is the employer’s responsibility to select the most qualified candidate for a position. The ADA makes it unlawful to discriminate against an individual with a disability who is qualified on the basis of a disability. Agencies must determine whether or not an individual with a disability is qualified at the time of the hiring decision, based on the person's present capabilities. Agencies should not make decisions based on speculation about what may happen in the future or concerns about increased insurance premiums or workers' compensation costs.

The appointing authority shall consider the essential functions of the position that have been identified when determining which applicant will be offered employment. If the disability of an applicant prevents or impedes the performance of one or more of the marginal functions of the position, the agency should not consider those functions when determining which applicant will be offered employment.

QUALIFICATION STANDARDS AND TESTS

It is unlawful for an employer to use qualification standards, employment tests or other selection criteria that screen out or tend to screen out an individual with disability or a class of individuals with a disability(s) on the basis of disability, unless the standard, test or other selection criteria, as used by the State or agency, is shown to be job-related for the position in question and is consistent

with business necessity. This provision is applicable to all types of selection criteria, including safety requirements, vision or hearing requirements, walking requirements, lifting requirements, and employment tests. Legitimate production standards will generally not be subject to a challenge under this provision.

Accommodations may be needed to assure that tests or examinations measure the actual ability of an individual to perform the essential functions, rather than reflecting limitations caused by a disability. Tests should be given to people who have sensory, speaking, or manual impairments in formats that do not require the use of their impaired skills; unless that is the job-related skill the test is designed to measure.

For example, an applicant for a position may have dyslexia, a learning disability, which causes difficulty in reading. The applicant may be given an oral rather than a written test, unless reading is an essential function of the position. Or the individual might be allowed more time to take a test, unless the test is designed to measure speed required for an essential function.

An employer has an obligation to inform applicants in advance that a test will be given, so that an individual who needs an accommodation can make such a request.

TRAINING

Individuals with disabilities must be provided equal access to training.

Reasonable accommodation should be provided, when needed, to individuals with disabilities to give them equal opportunity to benefit from training to perform their positions effectively and to advance in employment. An employer is responsible to provide reasonable accommodation whether the training occurs at the worksite or elsewhere.

EVALUATIONS, PERFORMANCE MANAGEMENT & DISCIPLINE

An employer can hold an employee with a disability to the same conduct standard (as long as it is job-related and consistent with business necessity) applied to employees without disabilities. For example, the ADA does not prevent an agency from maintaining a workplace free of violence or threats of violence, or from disciplining an employee who steals or destroys property. Thus, an employer may discipline an employee with a disability for engaging in such misconduct if it would impose the same discipline on an employee without a disability.

However, other conduct standards that are not be job-related for the position in question and consistent with business necessity an agency cannot discipline for or hold the individual accountable for. For example, an employee with a known psychiatric disability works in a warehouse loading boxes onto pallets for shipment. He has no customer contact and does not come into regular contact with other employees. Over the course of several weeks, he has come to work appearing increasingly disheveled. His clothes are ill-fitting and often have tears in them.

He also has become increasingly anti-social. Coworkers have complained that when they try to engage him in casual conversation, he walks away or gives a curt reply. When he has to talk to a coworker, he is abrupt and rude. However, his work has not suffered. The agency's policy states that employees should have a neat appearance at all times. The policy also states that employees should be courteous to each other. When told that he is being disciplined for his appearance and treatment of coworkers, the employee explains that his appearance and demeanor have deteriorated because of his disability, which was exacerbated during this time period. The dress code and coworker courtesy rules are not job-related for the position in question and consistent with business necessity because this employee has no customer contact and does not come into regular contact with other employees. Therefore, rigid application of these rules to this employee would violate the ADA.[6]

An employer can also hold an employee with a disability to the same production standards for performance of essential functions, with or without accommodation, as other similarly situated employees without disabilities. An agency can hold employees with disabilities to the same performance standards as other employees regarding marginal job functions, unless the disability affects the ability to perform these marginal functions. If the ability to perform marginal functions is affected by the disability, the agency must provide some type of reasonable accommodation, unless to do so would be an undue hardship.

An agency should not evaluate on a lower standard or discipline less severely employees with disabilities. However, an agency may not discipline or terminate an employee with a disability if the agency has refused to provide a requested reasonable accommodation that did not constitute an undue hardship, and the reason for unsatisfactory performance was the lack of accommodation.

REQUIRING "FULL RECOVERY" BEFORE RETURN TO WORK

An agency may not refuse to allow an individual with a disability to return to work on the basis that the employee is not fully recovered, unless he or she:

Caution:

The federal 9th Circuit Court of Appeals (which Nevada is a part of) has concluded that conduct resulting from a disability "is considered to be part of the disability, rather than a separate basis for termination." (Dark v. Curry Co. 451 F.3d 1078, 9th Cir. 2006) Additionally, the 9th Circuit has stated than a "decision motivated even in part by the disability is tainted and entitles a jury to find that an employer violated antidiscrimination laws." (Gambini v. Total Renal Care, Inc., 486 F.3d 1087, 9th Cir. 2007) It is suggested that agencies consult their agency's attorney before proceeding with discipline for misconduct that is directly related to an individual's disability.

- Cannot perform the essential functions of the position with or without reasonable accommodation; or
- Would pose a direct threat.

ADDRESSING GRIEVANCE(S)

The suggested procedure for handling ADA issues is through communication between the employee, supervisor and human resource staff.

An agency may have an ADA grievance policy in place; in which case, the procedures outlined may be used to resolve issues which have not been handled through communication between the parties.

Additionally, NAC 284.696 states that an employee alleging unlawful discrimination may:

- Report the alleged discrimination to:
  - The section of the Division of Human Resource Management that investigates discrimination (800-767-7381);
  - The Attorney General;
  - The employee's appointing authority;
  - An equal employment opportunity officer;
  - A human resource representative of the agency in which the employee is employed; or
  - The office charged with enforcing affirmative action within the appropriate university, state college or community college which is part of the Nevada System of Higher Education.
- Use the grievance procedure; or
- File a complaint with:
  - The Nevada Equal Rights Commission or
  - The United State Equal Employment Opportunity Commission.

POSTER

The ADA requires that agencies post a notice describing the provisions of the ADA, a poster is available from the EEOC. See the Poster Adviser on the Division of Human Resource Management's website for a link to the current version online. The notice must be made accessible to applicants and employees.

ACCOMMODATION PROCESS

The accommodation requirement is best understood as a means by which barriers to the equal employment opportunity of an individual with a disability are removed or alleviated.

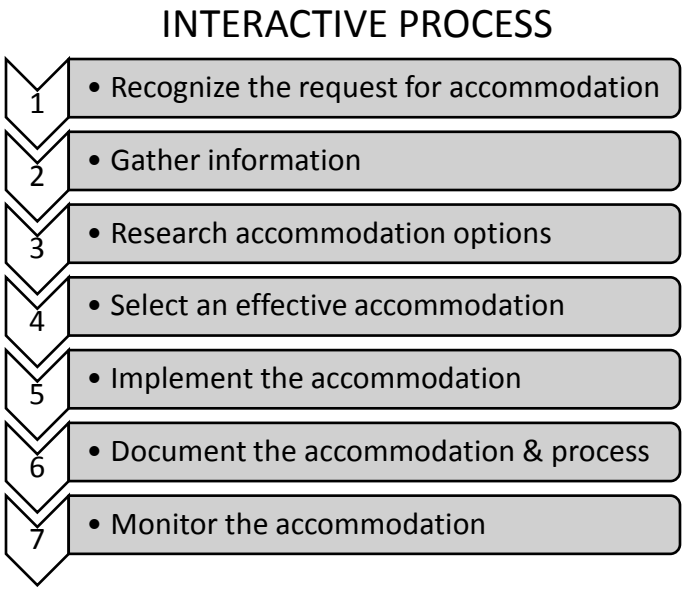
These barriers may be, but are not restricted to:

- Physical or structural obstacles that inhibit or prevent the access of an individual with a disability to job sites, facilities or equipment
- Rigid work schedules that permit no flexibility as to when work is performed or when breaks may be taken
- Inflexible job procedures that unduly limit the methods of communication that are used in the position or the way in which particular tasks are accomplished

An agency is obligated to make an accommodation only to the known limitations of an individual with a disability who is otherwise qualified. In general, it is the responsibility of the applicant or employee with a disability to inform the employer that an accommodation is needed to:

- participate in the application process;
- perform the essential job functions; and/or
- receive equal benefits and privileges of employment.

The ADA provides that an agency cannot require an individual with a disability who is qualified to accept an accommodation that is neither requested nor needed by the individual. However, if a necessary reasonable accommodation is refused, the individual potentially could be considered not qualified for the position if unable to perform the functions of the position.



An agency is not required to provide an accommodation if unaware of the need or disability. However, if an individual's need for accommodation is a) obvious and b) the individual's disability prevents the individual from requesting an accommodation; the agency must begin the accommodation process.

If an agency can grant requested assistance without further consideration, it is suggested

What if you are not sure if an individual is requesting an accommodation?

Ask the individual to clarify what is being requested and why.

that the assistance be provided without labeling it as an "accommodation". If requested assistance cannot be granted without further consideration, then the agency would need to proceed with the interactive process.

What is the interactive process? It can be described as a process to clarify what the individual needs and to identify a reasonable accommodation. Responsibility to move the interactive process forward rests on both the agency and individual. It is suggested to restrict communication to fact finding and problem resolution only and not to discuss performance problems as part of the interactive process.

Also keep in mind that certain steps in the interactive process may be taken at the same time or skipped (if the agency or individual already has addressed the issue).

RECOGNIZE THE REQUEST FOR ACCOMMODATION

What is a request for accommodation? Communication of a need for an “adjustment or change… for a reason related to a medical condition”.[4]

An individual may use “plain English" to request accommodation. An applicant or employee does not have to specifically request a "reasonable accommodation" or mention the "ADA”. A request for accommodation may be as simple as, "I need <accommodation> because of my <medical condition>".

However, just because an individual requests an accommodation, it is not a guarantee that the individual will be provided an accommodation or the specific accommodation requested. An individual with a disability should request a reasonable accommodation when he or she knows that there is a workplace barrier that is preventing him or her, due to a disability, from effectively competing for a position, performing the functions of a position, or gaining equal access to a benefit of employment. When an individual decides to request accommodation, the individual or his or her representative (e.g., family member, friend, health professional) must let the employer know that he or she needs an adjustment or change at work for a reason related to a medical

condition. Requests for reasonable accommodation do not need to be in writing. Individuals may request accommodation in conversation or may use any other method of communication.

GATHER INFORMATION

REVIEW ESSENTIAL FUNCTIONS

Review the Position Functions (ADA-3) to verify that they are correct and current. Do they accurately reflect the individual's position?

COMMUNICATE WITH INDIVIDUAL REGARDING IMPAIRMENT

Unless the individual's impairment is obvious, the agency may need to communicate with the individual regarding what his or her limitation(s) are and how long they will last. This communication may involve providing the individual with the position's essential functions and a list of questions for his or her health care provider.

HEALTH CARE PROVIDER

A health care provider can provide the facts necessary to establish whether an individual meets the definition of disability, whether an accommodation is necessary and may recommend an accommodation.

Agencies should provide health care providers who conduct an examination with information about the individual's job, specifically the essential functions. The Medical Inquiry in Response to an Accommodation Request form (NPD-86) has been developed as a template; however, the questions asked of the health care provider must be chosen and adapted based on the individual's specific circumstances. Also, information that has already been provided may not be requested again.

SECOND OPINION

The ADA does not prevent an employer from requiring an individual to go to an appropriate health professional of the employer's choice if the individual provides insufficient information from his treating

Keep in mind:

An employer may not ask for documentation when:

- Both the disability and the need for reasonable accommodation are obvious; or
- The individual has already provided the employer with sufficient information to substantiate that he or she has an ADA disability and needs reasonable accommodation.

An agency may not request complete medical records or health information unrelated to the disability.

health care professional to substantiate that he or she has an ADA disability and needs a reasonable accommodation. However, if an individual provides insufficient documentation in response to the agency's initial request, the agency should explain why the documentation is insufficient and allow the individual an opportunity to provide the missing information in a timely manner. Documentation is insufficient if it does not establish the existence (or not) of an ADA disability and explain the need for reasonable accommodation.

If an agency requires an employee to go to a health professional of the employer's choice, the agency must pay all costs associated with the visit(s). State administrative regulations provide a procedure for obtaining a second and third medical opinion, see NAC 284.566.

DOES THE INDIVIDUAL HAVE A COVERED DISABILITY?

It is the agency's responsibility to determine whether an individual meets the definition of disability under the ADA. The ADAAA states that this should not require extensive analysis.

IS THE INDIVIDUAL QUALIFIED?

This analysis is a two step inquiry. 1. Does the individual have the skills, experience, education and other job-related requirements (e.g., certification, licensure) of the position? 2. Can the individual perform the essential functions of the position with or without accommodation?

Future, potential difficulties may not be considered in deciding if an individual is qualified.

If an agency adjusts a position and its essential functions based upon business necessity, an individual may no longer be qualified. Also, if an individual poses a direct threat in that position, then the individual is not qualified.

DOES THE INDIVIDUAL POSE A DIRECT THREAT?

A direct threat is a significant risk ("a high, and not just a slightly increased, risk"[6]) of substantial harm to the health or safety of the individual or others that cannot be eliminated or reduced by reasonable accommodation. The risk must be specific, current (not speculative) and based on objective facts.

In determining whether an individual with a disability poses a direct threat, the factors to consider include:

- the duration of the risk;
- the nature and severity of the potential harm;
- the likelihood that the potential harm will occur; and

- the imminence of the potential harm.

DOES THE INDIVIDUAL NEED AN ACCOMMODATION?

Is the requested accommodation because of or related to the disability? An agency has a responsibility to provide accommodation for limitation(s) relating to a disability. It is not the agency's responsibility to provide accommodation to an individual with a disability if that accommodation will not compensate for the impairment affecting the employee's employment.

RESEARCH ACCOMMODATION OPTIONS

COMMUNICATION WITH INDIVIDUAL

In consultation with the individual to be accommodated, potential accommodations should be identified and assessed as to the effectiveness each would have in enabling the individual to perform the essential functions of the position. If this consultation with the individual does not reveal a potential reasonable accommodation, several other sources of information are available.

RESOURCES

There are various resources for researching potential accommodations, see Resources & References.

SELECT AN EFFECTIVE ACCOMMODATION

Once potential accommodations have been identified, the agency should assess the effectiveness of each potential accommodation in assisting the individual in need of the accommodation to:

- participate in the application process;
- perform the essential job functions; and/or
- receive equal benefits and privileges of employment.

If more than one accommodation will effectively enable the individual to perform the essential functions or if the individual would prefer to provide the accommodation, the preference of the individual should be given primary consideration. However, it should be noted that the agency is encouraged, but not obligated, to select the preference of the individual. The agency providing the accommodation has the ultimate discretion to choose between effective reasonable accommodations, and may choose a less expensive, easier to provide or less disruptive of agency operations reasonable accommodation. Accommodations should be considered on a case-by-case basis.

When selecting a reasonable accommodation the following factors should be considered:

- the individual's impairment(s);
- the position's essential functions;
- impact on workflow;
- applicable productivity standards; and
- interaction with co-worker(s).

IS THE ACCOMMODATION AN UNDUE HARDSHIP?

"**29 CFR §1630.2 Definitions**…

(p) *Undue hardship*—(1) *In general. Undue hardship* means, with respect to the provision of an accommodation, significant difficulty or expense incurred by a covered entity, when considered in light of the factors set forth in paragraph (p)(2) of this section.

(2) *Factors to be considered.* In determining whether an accommodation would impose an undue hardship on a covered entity, factors to be considered include:

(i) The nature and net cost of the accommodation needed under this part, taking into consideration the availability of tax credits and deductions, and/or outside funding;

(ii) The overall financial resources of the facility or facilities involved in the provision of the reasonable accommodation, the number of persons employed at such facility, and the effect on expenses and resources;

(iii) The overall financial resources of the covered entity, the overall size of the business of the covered entity with respect to the number of its employees, and the number, type and location of its facilities;

(iv) The type of operation or operations of the covered entity, including the composition, structure and functions of the workforce of such entity, and the geographic separateness and administrative or fiscal relationship of the facility or facilities in question to the covered entity; and

(v) The impact of the accommodation upon the operation of the facility, including the impact on the ability of other employees to perform their duties and the impact on the facility's ability to conduct business."

The general principle is that an accommodation does not have to be offered if it is an undue hardship for the State of Nevada. Although the full resources of the State of Nevada, not just the

unit the employee is in, would be considered when making this decision, agency management and the Department of Administration's Budget Division may need to be consulted.

A potential negative effect on the morale of other employees is not an undue hardship.

IMPLEMENT THE ACCOMMODATION

When offering a reasonable accommodation, it is suggested to explain the reason that particular accommodation is being offered (especially if it is not the accommodation that the individual requested). The Agency Response form (NPD-87) documents the decision in writing.

Proceed with implementing the accepted reasonable accommodation as soon as possible.

DOCUMENT THE ACCOMMODATION & PROCESS

If the interactive process breaks down, liability under the ADA will rest on whoever (employer or individual) did not meet their obligations in the process. Documentation will assist an agency in establishing that it fulfilled its obligations in the process.

It is recommended to write a summary of any meetings, submit a copy to attendees asking for revisions/corrections, finalize and then redistribute to all attendees. Summaries of any analysis and records of any research, printouts or notes from conversations should also be kept as documentation. And most importantly, there should be documentation outlining the final decision regarding any accommodation or decision against providing accommodation and the individual's response to an offer of reasonable accommodation. See Confidentiality for the guidelines on storage of documents containing medical information.

MONITOR THE ACCOMMODATION

An agency should follow up with an individual regarding the effectiveness of a reasonable accommodation. The follow up should be scheduled, performed and documented. The length of time between follow ups will depend on the type of accommodation provided. Follow ups should include communication with the individual.

If the follow up indicates that the reasonable accommodation is not allowing the individual to participate in the application process, perform the essential job functions or receive equal access to benefits and privileges of employment, the agency should re-enter the interactive process with the individual.

TYPES OF ACCOMMODATION

ACCESSIBILITY

Employment activities must take place in an integrated setting. Employees with disabilities may not be segregated into particular facilities or parts of facilities. This means that architectural barriers might have to be removed or altered to provide structural accessibility to the workplace. However, an employer is not required to make structural modifications that are unreasonable and would impose an undue hardship.

In existing structures, structural modifications are necessary to the extent that they will allow an employee with a disability to perform the essential functions of the job including access to work stations and normal support facilities such as bathrooms, water fountains, and lunchrooms.

The State Public Works Division may be able to provide limited consultation regarding accessibility issues, see the Resources page for contact information.

POSITION RESTRUCTURING

Position restructuring as a reasonable accommodation may involve reallocating or redistributing the marginal functions of a position. An agency is not required to reallocate essential functions of a job as a reasonable accommodation. Essential functions, by definition, are those that a qualified individual must perform, with or without accommodation.

For example, firefighters are required to pass an annual physical agility test, which would include a lifting requirement, upon employment and annually thereafter as an essential function of the position. If an individual became disabled and could no longer meet the lifting requirement, it would not be reasonable to remove this test as it is essential to the job.

Although an agency is not required to reallocate essential job functions, it may be a reasonable accommodation to change when or how the essential functions are performed. For example:

- Reassigning duties among co-workers. For example, if an administrative assistant had a vision impairment that prevented him or her from typing in small spaces on forms, whenever such forms needed to be prepared, the marginal function might be assigned to another administrative assistant without a visual impairment. In exchange, the administrative assistant with a disability could assume one of the other administrative assistant's marginal functions, such as filing.

- Eliminate non-essential tasks. For example, if a duty(s) of the position is not necessary, it could be eliminated entirely. A mail clerk, rather than traveling to the post office in the early morning, might be allowed to wait for regular mail delivery.

- Reassign visits to accessible sites. For example, a repair person who uses a wheelchair could service the accessible sites, while the other sites could be assigned to someone without a mobility impairment.
- Allow work in other than the traditional office setting. For example, a telephone surveyor could make calls on a designated line from home instead of having to come regularly to an inaccessible office to make the calls.
- Assign uninterrupted work times for particular tasks. For example, an individual with a learning disability may have problems when his or her attention is interrupted. Scheduling uninterrupted work time might allow greater concentration and heighten the performance of such an individual.

LEAVE

Flexible leave policies should be considered as a reasonable accommodation when an individual with a disability requires time off from work because of his or her disability. An agency is not required to provide additional paid leave as an accommodation, but should consider allowing use of accrued leave or leave without pay, where this will not cause an undue hardship. Such employees may meet the eligibility requirements of the Family and Medical Leave Act and the rights and benefits under this law need to be considered, see the FMLA Overview.

How much leave is reasonable? The length of the leave granted will depend on the employee's disability and position. Most courts and the EEOC have indicated that indefinite leave is not reasonable. Also, providing leave for unpredictable attendance is generally not considered reasonable under the ADA.

MODIFICATION OF WORK SCHEDULE

Many people with disabilities are fully qualified to perform jobs with the accommodation of a modified work schedule (e.g., a schedule other than a standard 8:00 a.m. to 5:00 p.m. workday or a standard Monday to Friday workweek). Depending on the nature of the work assignment and operational requirements, modifications to work schedules and hours may be a reasonable accommodation as long as it does not result in an undue hardship. Modified work schedules may include flexibility in work hours, the workweek, or part-time work. For example:

- An employee who is unable to drive at night (e.g., an employee with poor night vision) could be assigned day-shift work.
- An employee may need additional rest periods (e.g., employees diagnosed with multiple sclerosis, cancer, diabetes, respiratory conditions, mental illness).

- An employee with mobility or other impairments may find it difficult to use public transportation during peak hours, or may depend upon special para-transit schedules.
- An employee who needs kidney dialysis treatment may be unable to work two days per week because treatment is only available during work hours on weekdays.

AUXILIARY AIDS

Some examples of auxiliary aids are interpreters, note takers, computer-aided transcription services, written materials, exchange of written notes, telephone handset amplifiers, assistive listening systems, telephones compatible with hearing aids, closed caption decoders, open and closed captioning, text telephones (TTYs), videotext displays, video interpreting services (VIS), accessible electronic and information technology, readers, taped texts, audio recordings, Braille materials and displays, screen reader software, magnification software, optical readers, secondary auditory programs (SAP) and large print materials.

INTERPRETERS

"Effective October 1, 2008, regulations for the fields of Interpreting for the Deaf and CART (Computer Aided Realtime Translation) were developed. These regulations require providers of Interpreting/CART to be registered with the State of Nevada in order to legally perform CART or Interpreting in the State of Nevada."[10] The Department of Health and Human Services, Aging and Disability Services Division maintains a list of registered CART/Interpreters on their website.

MODIFICATION OR PURCHASE OF EQUIPMENT OR DEVICES

Purchase of equipment or modifications for existing equipment may be an effective accommodation for an employee to overcome existing barriers in performing the functions of a position. These devices range from very simple solutions, such as an elastic band that can enable a person with cerebral palsy to hold a pencil and write, to electronic equipment that can be operated with eye or head movements by people who cannot use their hands. Other types of equipment and devices that may be appropriate include, but are not limited to:

- Telephone headsets and adaptive light switches;
- Speakerphones;
- A supportive desk chair;
- A raised desk;
- Modified equipment controls for hand or foot operation;
- Keyboard hand rest and a finger guide mounted on equipment;

- Armrest attachments; or
- Buzzers to replace warning lights.

An agency is only obligated to provide equipment that is needed to perform a job; generally, there is no obligation to provide equipment that the individual uses regularly in daily life (e.g., hearing aid, wheelchair).

However, an agency may be obligated to provide items of this nature if special adaptations are required to perform a job. For example, an employee with a mobility impairment may own and use a manual wheelchair. If the employee's job requires movement between buildings that are widely separated and the employee's mobility impairment prevents operation of a wheelchair manually for that distance, or if heavy, deep-pile carpeting prevents operation of a manual wheelchair, then it may be a reasonable accommodation to provide an employee with a motorized wheelchair.

MODIFICATION OF WORK ENVIRONMENT

MODIFICATION OF POLICIES AND/OR PROCEDURES

Modifications or adjustments in the ways that tests and training are administered or revisions to other employment policies and practices may be reasonable accommodations to provide equal employment opportunities for individuals with disabilities.

Modifications to policies and procedures may include:

- Modifying a policy prohibiting animals in the workplace, so that a person with a disability may be accompanied by a service animal (dog or miniature horse[12])
- Modifying an emergency evacuation procedure to provide effective evacuation for individuals with difficulty in mobility in case of emergency
- Providing accessible parking for an individual with a qualified sticker, license plate or placard

When the accommodation provided for an individual with a disability is the modification of a policy, the agency may still continue to apply the policy to all other employees.

TELECOMMUTING

The EEOC has stated that telecommuting is a potential reasonable accommodation if it is effective and does not constitute an undue hardship.[9] However, some questions to be considered when deciding whether telecommuting is a reasonable accommodation are:

- Is teamwork an essential function of the position?
- Does the position require the individual to be physically present?
- Does the individual need physical access to documents and information?
    - Are any of the documents or information confidential?
- Does the position have clearly defined and measurable work activities?
- Does the position need close supervision?
- Does the position require special equipment?

REASSIGNMENT

Before considering reassignment of an employee to a vacant position, accommodations that will allow the employee to remain in his or her position should be considered. Reassignment is only required for current employees, not prospective employees. The State is not required to consider a different position for a job applicant who is not able to perform the essential functions of a position, with or without reasonable accommodation. Reassignment to a vacant position cannot be denied based on the fact that the individual is not a permanent employee. However, if the employee never adequately performed the essential functions with or without reasonable accommodation, reassignment is not necessary as the individual was never qualified.

Reassignment may not be used to limit, segregate, or otherwise discriminate against an employee with a disability. An agency may not reassign people with disabilities only to certain undesirable positions, or only to certain offices or facilities.

Appendix to Title 29, Part 1630—Interpretive Guidance on Title I of the Americans with Disabilities Act

"The appropriate reasonable accommodation is best determined through a flexible, interactive process that involves both the employer and the individual with a disability…

When an individual with a disability has requested a reasonable accommodation to assist in the performance of a job, the employer, using a problem solving approach, should:

(1) Analyze the particular job involved and determine its purpose and essential functions;

(2) Consult with the individual with a disability to ascertain the precise job-related limitations imposed by the individual's disability and how those limitations could be overcome with a reasonable accommodation;

(3) In consultation with the individual to be accommodated, identify potential accommodations and assess the effectiveness each would have in enabling the individual to perform the essential functions of the position; and

(4) Consider the preference of the individual to be accommodated and select and implement the accommodation that is most appropriate for both the employee and the employer…"

Reassignment shall be made to a position equivalent to the one presently held in terms of pay, privileges, benefits, geographical location and responsibilities, if the individual is qualified for the new position and if such a position is vacant or will be vacant within a reasonable amount of time unless it is demonstrated that such an appointment would cause an undue hardship to the appointing authority. A "reasonable amount of time" should be determined on a case-by-case basis.

An employee must be “qualified” for the new position. An employee is “qualified” for a position if the employee:

1. Satisfies the requisite skill, experience, education, and other job-related requirements of the position; and

2. Can perform the essential functions of the new position, with or without reasonable accommodation.

The employee does not need to be the best-qualified individual for the position in order to obtain it as a reassignment. An employee being reassigned does not have to compete for a position if it is equivalent or a lower grade than the employee’s current position.

The State of Nevada shall offer to reassign an individual to an equivalent position in a different geographical location if there are no equivalent positions vacant or soon to be vacant in the same geographical location.

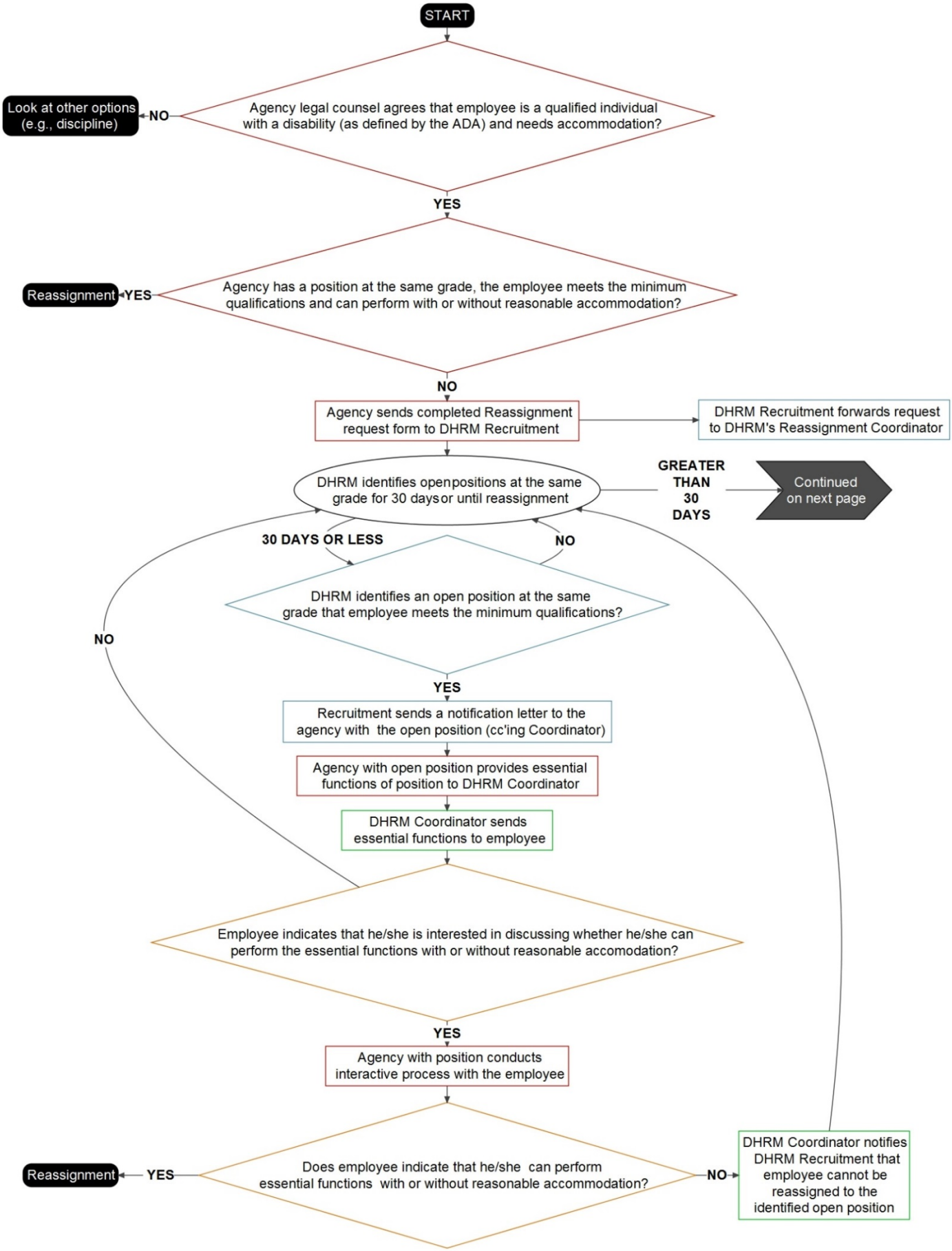
The State of Nevada shall offer to reassign an individual to a lower graded position (unless it is demonstrated that such an appointment would cause an undue hardship to the appointing authority) if there are no reasonable accommodations that would enable the employee to remain in the current position and there are no equivalent positions vacant or soon to be vacant for which the employee is qualified (with or without an reasonable accommodation). In such a situation, the State does not have to maintain the individual's salary at the level of the higher graded position. Refer to the rules governing compensation in the Rules for State Personnel Administration for how to calculate pay in the case of a voluntary demotion.

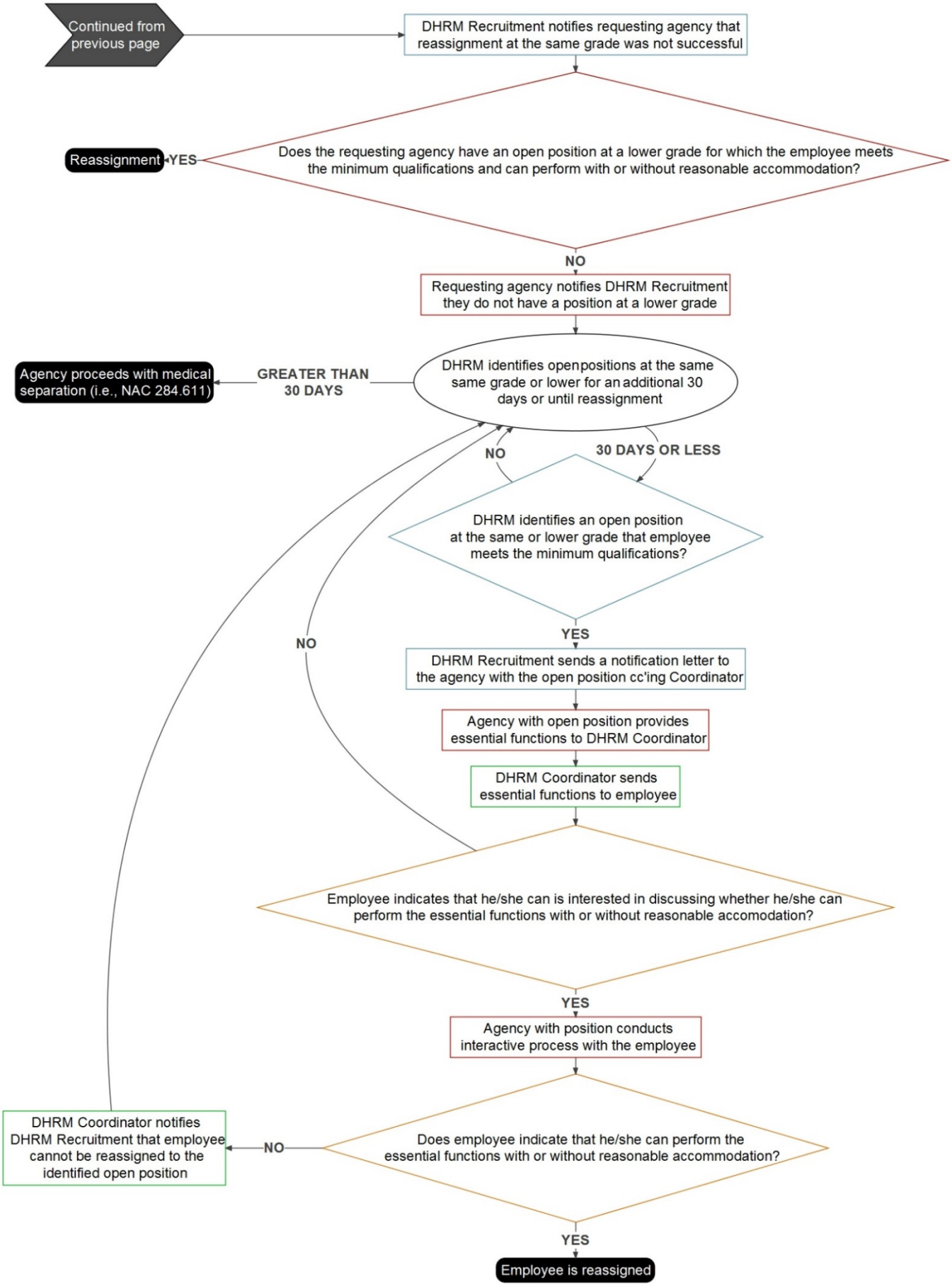
If there is more than one vacancy for which the employee is qualified, the State must place the individual in the position that comes closest to the employee’s current position in terms of pay, status, privileges and responsibilities. If it is unclear which position comes closest, the employee should be consulted about his or her preference before determining the position to which the employee will be reassigned. Reassignment does not include giving an employee a promotion; thus, an employee must compete for any vacant position that would constitute a promotion.

The State of Nevada is not required to create a new job or to bump another employee from a job in order to provide reassignment as a reasonable accommodation.

(Sections 2 – 4 of LCB File No. R097-16, 11-2-2016)

REASSIGNMENT PROCESS




Continued from previous page
DHRM Recruitment notifies requesting agency that reassignment at the same grade was not successful
Reassignment
YES
Does the requesting agency have an open position at a lower grade for which the employee meets the minimum qualifications and can perform with or without reasonable accommodation?
NO
Requesting agency notifies DHRM Recruitment they do not have a position at a lower grade
Agency proceeds with medical separation (i.e., NAC 284.611)
GREATER THAN 30 DAYS
DHRM identifies openpositions at the same same grade or lower for an additional 30 days or until reassignment
NO
30 DAYS OR LESS
DHRM identifies an open position at the same or lower grade that employee meets the minimum qualifications?
YES
NO
DHRM Recruitment sends a notification letter to the agency with the open position cc'ing Coordinator
Agency with open position provides essential functions to DHRM Coordinator
DHRM Coordinator sends essential functions to employee
Employee indicates that he/she can is interested in discussing whether he/she can perform the essential functions with or without reasonable accomodation?
YES
Agency with position conducts interactive process with the employee
DHRM Coordinator notifies DHRM Recruitment that employee cannot be reassigned to the identified open position
NO
Does employee indicate that he/she can perform the essential functions with or without reasonable accommodation?
YES
Employee is reassigned

FUNDING

The cost of accommodation does vary; however, the majority of accommodations can be provided at little or no cost.

Once the appropriate accommodation is identified, in consultation with the individual in need of the accommodation, an employer should work with their assigned Budget Analyst to determine appropriate State funding sources.

In addition, the U.S. Department of Veterans Affairs may provide financial assistance to disabled veterans for equipment needed to help perform jobs. Some organizations that serve people with particular types of disabilities also provide financial assistance for needed accommodations. Other types of assistance may be available in the community such as transportation services.

Also, the applicant or employee may be willing to share in the cost of the accommodation, which is an undue hardship on the State, or may already own the equipment or assistive device necessary to perform the essential functions of the job.

CONFIDENTIALITY

All information obtained from medical examinations and inquiries must be collected and maintained on separate forms, in separate secure medical files and must be treated as confidential medical records per NAC 284.726.

All medical-related information must be kept confidential, with the following exceptions:

- Supervisors and managers may be informed about necessary restrictions on the work or duties of an employee and necessary accommodations;
- First aid and safety personnel may be informed, when appropriate, if the disability might require emergency treatment;
- Government officials investigating compliance with the ADA must be given relevant information upon request;
- Relevant information may be provided to state workers' compensation offices, "second injury" funds and workers' compensation insurance carriers in accordance with state workers' compensation laws; or
- Relevant information may be provided to insurance companies where the company requires a medical examination to provide health or life insurance for employees.

DEALING WITH RESPONSES FROM CO-WORKERS

Other employees may at times perceive an individual as being given preferential treatment. However, others (including co-workers) may not be told that the individual is receiving a reasonable accommodation because this would usually amount to a disclosure that the individual has a disability.

As long as there is no coercion by the employer, an individual with a disability may voluntarily choose to disclose to coworkers his or her disability and/or the fact that he or she is receiving a reasonable accommodation.

What can a supervisor or human resources say when co-workers ask about another employee's accommodation?

"The State's policy is to assist individuals who encounter difficulty in the workplace. However, many workplace issues encountered by individuals are personal and, in those circumstances, it is the State's policy to respect an individual's privacy. Your privacy would also be respected if you found it necessary to ask for some kind of workplace change for personal reasons.[4]

OTHER LAWS & PROVISIONS

FAMILY AND MEDICAL LEAVE ACT (FMLA)

The FMLA and the ADA both potentially grant an employee leave in certain circumstances. Under the ADA, unpaid (though applicable paid may be used) leave may be an accommodation and may be provided to an individual with a disability who is otherwise qualified when it is reasonable and unless (or until) it imposes an undue hardship on the operation of the employer's business. Under the FMLA, an "eligible" employee may take leave for a qualifying event, as outlined in the FMLA Overview.

At the end of FMLA leave, an agency must return the employee to the same or an equivalent job. An employee with an ADA disability who is granted leave as a reasonable accommodation is entitled to return to his or her same position unless the agency demonstrates that holding open the position would impose an undue hardship or an employee is no longer qualified to return to his or her original position. If both laws apply, the agency must provide the employee with the greater benefit and restore the employee to his or her same position absent undue hardship.

Not all employees protected by the ADA are entitled to leave under the FMLA. Employees protected by the ADA must be independently determined to be eligible for FMLA coverage. An FMLA "serious health condition" is not necessarily an ADA "disability" and an ADA "disability" is not necessarily an FMLA "serious health condition". In addition, the fact that an individual has a record of a "serious health condition" does not necessarily mean that he or she has a record of an ADA disability.

When an employee requests leave under the FMLA for a "serious health condition", an agency will not violate the ADA by asking for the information specified in a FMLA certification form. An agency is entitled to know why an employee, who otherwise should be at work, is requesting leave as allowed under the FMLA. If the inquiries are strictly limited in this fashion, they would be "job-related and consistent with business necessity" under the ADA.

The FMLA limitation on the number of workweeks of leave taken does not mean that the ADA also limits employees to a specific number of workweeks of leave per year. An individual with a disability who is otherwise qualified may be entitled to more than 12 weeks of unpaid leave as an accommodation if the additional leave is reasonable and will not impose an undue hardship on the operation of the agency's business.

GENETIC INFORMATION NONDISCRIMINATION ACT (GINA)

GINA defines genetic information as including, "information about an individual's genetic tests and the genetic tests of an individual's family members, as well as information about any disease,

disorder, or condition of an individual's family members (i.e. an individual's family medical history)."[7]

GINA prohibits requesting or receiving genetic information. Genetic information may be provided by a health care provider in response to medical inquiries as part of the ADA's interactive process. If an employee and/or his or her health care provider is warned not to provide genetic information, receipt of genetic information is not a violation of GINA. The EEOC's Regulations Under the Genetic Information Nondiscrimination Act of 2008 provides the following sample language to be included with requests for medical information:

> ''The Genetic Information Nondiscrimination Act of 2008 (GINA) prohibits employers and other entities covered by GINA Title II from requesting or requiring genetic information of an individual or family member of the individual, except as specifically allowed by this law. To comply with this law, we are asking that you not provide any genetic information when responding to this request for medical information. 'Genetic information' as defined by GINA, includes an individual's family medical history, the results of an individual's or family member's genetic tests, the fact that an individual or an individual's family member sought or received genetic services, and genetic information of a fetus carried by an individual or an individual's family member or an embryo lawfully held by an individual or family member receiving assistive reproductive services.''"[7]

The EEOC has stated that genetic information may be kept with other medical information in compliance with the ADA's rules on medical records confidentiality.

HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT (HIPAA)

Title IV of the Act defines rules for protection of patient information. Health care providers, health organizations, and government health plans that use, store, maintain, or transmit patient health care information are required to comply with the privacy regulations of HIPAA. It sets limits on the use and release of health records and establishes safeguards to protect the privacy of health information. In general, a health care provider or plan may not use or disclose an individual's healthcare information without the patients permission except for treatment, payment or healthcare operations. Typically, most agencies, in regards to their employees, are not covered by HIPAA regulations. The requirements of the HIPAA Privacy Rule can apply when an employee's medical information is requested from a HIPAA-covered health care provider. Regardless of whether HIPAA applies in the situation, medical information must be kept confidential and separate from other personnel records.

WORKERS' COMPENSATION

The purpose of workers' compensation is to provide a system for securing prompt and fair settlement of employees' claims against employers for occupational injury and illness. Whereas, the purpose of the ADA is to remove barriers which prevent qualified individuals with disabilities from enjoying the same employment opportunities that are available to persons without disabilities.

Whether an injured worker is protected by the ADA will depend on whether or not the individual meets the ADA definition of an individual with a disability who is qualified.

EARLY RETURN-TO-WORK PROGRAM

The State of Nevada has established an Early Return-to-Work Program to enhance recovery, help minimize workers' compensation costs and provide a service to employees who are injured or contract an occupational disease in the course and scope of their employment with the State. Employees will be placed in temporary modified duty positions, when feasible, during the course of recovery from an injury or occupational disease that precludes them from performing their normal job tasks. In the event of a permanent disability that prevents an employee from performing the essential functions of his or her regular position and for which reasonable accommodation cannot be made, every effort will be made to place the employee in an alternative vacant position that he or she is qualified to perform and that matches his or her physical limitations. See the Early Return-to-Work Program, A Guide for Managers, Supervisors and Personnel Representatives for additional information. The Risk Management Division serves as a technical resource for the Early Return-to-Work Program. Call (775) 684-3187 for information or assistance.

VOCATIONAL REHABILITATION

Vocational rehabilitation is a State and federally funded program to help eligible individuals with disabilities obtain or retain a job. As appropriate to the vocational rehabilitation needs of each client and consistent with the individual's informed choice, vocational rehabilitation provides assessment and evaluation, counseling and guidance, training, interpretation, and other goods and services to allow an individual with a disability who is qualified to become employed or retain employment. The Rehabilitation Division of the Department of Employment, Training and Rehabilitation may be able to provide agencies with consultation in the accommodation process. See Resources for the Rehabilitation Division's contact information.

SEPARATION FOR PHYSICAL, MENTAL OR EMOTIONAL DISORDER (NAC 284.611)

NAC 284.611 allows for the separation of an employee for physical, mental or emotional disorder; however, the regulation outlines specific steps that must be taken before proceeding with this action. One of the steps is "determine whether reasonable accommodation can be made to enable the employee to perform the essential functions of his job".

700-HOUR STATUTE

The 700-Hour statute requires agencies to make temporary limited appointment of 700 hours' duration of individuals with disabilities. Individuals must be certified by the Rehabilitation Division of the Department of Employment, Training and Rehabilitation (see Resources for contact information in both northern and southern Nevada), possess the training and skills necessary for the position, and be able to perform the essential functions of the position with or without reasonable accommodation.

Once employed, the 700 hours of work experience are used to measure the individual's merit and fitness for the job. At the end of the appointment, if the individual's performance is satisfactory, he or she may continue in the position as a regular employee with the 700 hours counting toward the time required to earn permanent status.

A probationary or permanent employee who occupies a permanent full-time position is not eligible for the provisions of this section unless his or her disability jeopardizes his or her continued employment in his or her present position and placement on the list does not merely circumvent the provisions of the Rules for State Personnel Administration governing promotion or transfer, see NRS 284.327 and NAC 284.364.

NEVADA PREGNANT WORKERS' FAIRNESS ACT

Upon request, an employee must be provided reasonable accommodations relating to her pregnancy, childbirth, or a related medical condition unless the accommodation would impose an undue hardship.

RESOURCES & REFERENCES

RESOURCES

Resource	Website/email address	Phone number(s)
AbleData	http://www.abledata.com	
AccessibleTech.org	http://www.accessibletech.org	
ADA Home Page	http://www.ada.gov	
Bureau of Vocational Rehabilitation, Nevada Department of Employment, Training & Rehabilitation	http://www.detr.state.nv.us/Rehab%20pages/voc%20rehab.htm	S. NV: (702) 486-5230 N. NV: (775) 684-4040 S. NV TTY: (702) 486-1018 N. NV TTY: (775) 684-8400
Division of Human Resource Management	http://hr.nv.gov	(775) 684-0111
Disability and Business Technical Assistance Centers (DBTAC): Pacific ADA Center	http://www.adapacific.org	

Resource	Website/email address	Phone number(s)
The Job Accommodation Network	http://www.askJAN.org	Voice (800) 526-7234 TTY (877) 781-9403
National Center for the Dissemination of Disability Research	http://www.ncddr.org	
The National Organization on Disability	http://www.nod.org	
Nevada PEP	http://www.nvpep.org	
Public Works Division	http://spwb.state.nv.us/	(775) 684-4141
Registry of Interpreters for the Deaf	http://www.rid.org/	(301) 608-0050
RESNA Technical Assistance Project	http://www.resna.org/	Voice (703) 524-6686 TTY (703) 524-6639
Risk Management Division, Department of Administration (workers' compensation)	http://risk.state.nv.us	(775) 687-3187

U.S. Equal Employment Opportunity Commission	http://www.eeoc.gov/	Voice (800) 669-3362 TTY (800) 800-3302

REFERENCES

[1] ADA Amendments Act of 2008, Public Law 110-325, September 25, 2008

[2] U.S. Equal Employment Opportunity Commission, Regulations to Implement the Equal Employment Provisions of the Americans with Disabilities Act, as Amended, Final Rule, Federal Register, Vol.76, No. 58

[3] U.S. Equal Employment Opportunity Commission, Enforcement Guidance: Disability-Related Inquiries and Medical Examinations of Employees under the Americans with Disabilities Act (ADA), Number 915.002, 7/27/00

[4] U.S. Equal Employment Opportunity Commission, Enforcement Guidance: Reasonable Accommodation and Undue Hardship under the Americans with Disabilities Act, Number 915.002, 10/17/02

[5] U.S. Equal Employment Opportunity Commission, Questions and Answers about the Association Provision of the Americans with Disabilities Act, http://www.eeoc.gov/facts/association_ada.html

[6] U.S. Equal Employment Opportunity Commission, Enforcement Guidance on the Americans with Disabilities Act and Psychiatric Disabilities, Number 915.002, 3/25/97

[7] U.S. Equal Employment Opportunity Commission, Regulations Under the Genetic Information Nondiscrimination Act of 2008, Final rule, Federal Register, Vol. 75, No. 216

[8] U.S. Equal Employment Opportunity Commission, Enforcement Guidance: Workers' Compensation and the ADA, Number 915.002

[9] U.S. Equal Employment Opportunity Commission, Work At Home/Telework as a Reasonable Accommodation, http://www.eeoc.gov/facts/telework.html (last modified October 27, 2005)

[10] Department of Health and Human Services, Division of Aging and Disability, Office of Disability Services website, http://dhhs.nv.gov/Qry_CartInt_Registered.asp (accessed 7/6/11)

[11] The Americans with Disabilities Act of 1990 and Injured Workers. (1997, 2001) [Brochure] Cornell University, Bruce Growick (http://digitalcommons.ilr.cornell.edu/cgi/viewcontent.cgi?article=1027&context=edicollect, accessed 7/26/11)

[12] Department of Justice, Civil Rights Division, Nondiscrimination on the Basis of Disability in State and Local Government Services, Final Rule, Federal Register, Vol. 75, No.178

[13] ADA Update on Medical Examinations and Disability-Related Inquiries, National Employment Law Institute, David K. Fram Esq., April 2013

State of Nevada
Executive Branch

SEXUAL HARASSMENT AND DISCRIMINATION POLICY

Sexual harassment and discrimination based on race, color, national origin, religion, sex, age, disability, pregnancy, sexual orientation, genetic information, gender identity or expression, domestic relations[1] or compensation or wages[2] in any term, condition or privilege of employment are violations of State and/or federal law.

I. PURPOSE

The purpose of this Policy statement regarding sexual harassment and discrimination is to clearly express the position of the State of Nevada that all employees have the right to work in an environment free from all forms of discrimination and conduct which can be considered harassing, coercive or disruptive.

Sexual harassment and discrimination are forms of misconduct that undermine the integrity of the employment relationship. No employee, either male or female, should be subjected to unsolicited and unwelcomed sexual overtures or conduct, either verbal, written (including digital media, i.e., email, text or digital photos or graphics) or physical. No employee should experience discrimination in hiring, promotion, discharge, pay, fringe benefits, job training, classification, referral, and other aspects of employment. Sexual harassment and discrimination are personally offensive, debilitate morale, and, therefore, interfere with work effectiveness. An employee who engages in discriminatory behavior, or behavior that constitutes sexual harassment, may be subject to disciplinary action up to and including dismissal.

II. COVERAGE

This Policy is intended to be applicable to all State employees, officers, appointees such as board members, and volunteers in the executive branch of government. All elected officers are encouraged to adopt this Policy within their agencies.

[1] AB 229 (2017); AB 227 (2017).
[2] NRS 613.330.

III. RESPONSIBILITY

A. Sexual harassment and discrimination, whether committed by a supervisor, coworker, or member of the public is specifically prohibited as unlawful and against State policy. Appointing authorities are responsible for taking immediate and corrective action in response to complaints, regardless of whether the specific acts complained of were sanctioned or specifically forbidden and regardless of the manner in which the appointing authority becomes aware of the conduct.

B. Appointing authorities must ensure that each employee is provided with a copy of this Policy informing them that sexual harassment and discrimination are prohibited conduct and will not be tolerated or condoned. All employees will acknowledge receipt and understanding of the Policy through a signed statement.

C. All new employees, officers, appointees, board members and volunteers in the executive branch shall attend sexual harassment prevention training within six months of their appointment. Thereafter, employees are required to complete sexual harassment prevention refresher training once every two years.

D. Managers and supervisors are also required to attend additional training related to equal employment opportunity within 12 months of supervisory appointment and every three years thereafter.

E. Appointing authorities shall advise all employees of their responsibility to report incidents of sexual harassment and discrimination.

F. Appointing authorities shall designate employees within each agency to act as coordinators for the reporting of complaints of sexual harassment or discrimination and will notify employees and the Sexual Harassment/Discrimination Investigation Unit of the coordinator's name and contact information.

G. Supervisors shall have a complete understanding of this Policy. Supervisors who willfully disregard incidents of sexual harassment or discrimination by subordinates may be subject to discipline. Supervisors are responsible for ensuring their employees have received training as outlined in this Policy.

H. It is the responsibility of appointing authorities to make sure their agencies are in full compliance with this Policy and associated legal guidelines.

IV. STATE EMPLOYEES' RIGHTS AND RESPONSIBILITIES

A. Employees are entitled to work in a workplace free of sexual harassment and discrimination.

B. Employees are responsible for ensuring they do not sexually harass or discriminate against any other employee, client, applicant for employment, or other individual(s).

C. Employees are responsible for cooperating in the investigation of any complaint of alleged sexual harassment or discrimination. Employees are additionally responsible for cooperating with the efforts of their agency, division, board or commission to prevent and eliminate sexual harassment and discrimination and for maintaining a working environment free from such unlawful conduct. Pursuant to NAC 284.650, failure to participate in any investigation of alleged discrimination, including without limitation, an investigation of sexual harassment is cause for disciplinary action.

V. LEGAL DEFINITIONS AND GUIDELINES

A. NAC 284.771 specifies that sexual harassment violates the policy of this State and is a form of unlawful discrimination based on sex under State and federal law. An employee shall not engage in sexual harassment against another employee, an applicant for employment, or any other person in the workplace.

Sexual harassment is a very serious disciplinary infraction. An appointing authority may impose harsh disciplinary sanctions on persons who commit sexual harassment, even on first-time offenders.

B. As used in Section 703 of Title VII of the Civil Rights Act of 1964, "sexual harassment" means unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature when:

1. Submission to such conduct is made either explicitly or implicitly a term or condition of a person's employment; or

2. Submission to or the rejection of such conduct by a person is used as the basis for employment decisions affecting that person; or

3. Such conduct has the purpose or effect of unreasonably interfering with a person's work performance or creating an intimidating, hostile or offensive work environment. 29 C.F.R. § 1604.11.

C. Equal opportunity with regard to the terms, conditions and privileges of employment is mandated under Title VII of the Civil Rights Acts of 1964, the Americans with Disabilities Act of 2008, the Age Discrimination in Employment Act of 1967, the Equal Pay Act of 1963, Genetic Information Nondiscrimination Act of 2008, NRS 631.330, NRS 281.370, and numerous sections of Chapter 284 of the NRS which address the State's Personnel System.

D. The State of Nevada is an equal opportunity employer and does not discriminate against job applicants or employees based on race, color, religion, sex, national origin, disability, age, pregnancy, sexual orientation, genetic information, gender identity or expression, domestic relations, or compensation or wages.

E. Federal law prohibits retaliation against employees who bring sexual harassment or discrimination charges or assist in investigating such charges. Any employee making sexual harassment or discrimination complaints or assisting in the investigation of such a complaint will not be adversely affected in terms or conditions of employment, nor discriminated against, disciplined or discharged because of the complaint.

VI. PROCEDURE

A. Employee

1. Employees who believe they have been subjected to or witnessed sexual harassment or discrimination are encouraged to advise the person believed to have engaged in sexual harassment or discrimination that the conduct is unwelcome, undesirable or offensive. If the employee elects not to confront the alleged harasser or if the conduct persists after an objection, the employee shall report the incident to their supervisor or next level authority, or the employee may elect to report the incident as set forth below. Employees will be asked to complete a complaint form.

2. Employees may report incidents of sexual harassment or discrimination (a) to the coordinator within their agency designated to receive such complaints, or (b) by filing a complaint in NEATS on the Home Page, under Personal Tasks, "File a Sexual Harassment or Discrimination Complaint," or (c) by completing an NPD-30 Sexual Harassment or Discrimination Complaint Form located on the Division of Human Resource Management website, or (d) by calling the Division of Human Resource Management's Harassment/Discrimination Hotline at (800) 767-7381. Employees are always entitled to consult an attorney or labor representative or to report the incident to the Nevada Equal Rights Commission or the Equal Employment Opportunity Commission.

3. Employees should give the completed complaint form and any supporting documentation to the coordinator designated within their agency to receive such complaints or to the assigned investigator(s).

B. Appointing Authorities

1. After receiving notification of an employee's complaint, the appointing authority shall promptly notify the agency's assigned personnel, Deputy Attorney General or staff counsel assigned to represent the agency pursuant to State Administrative Manual § 1702 (legal counsel) and the Division of Human Resource Management's Sexual Harassment/Discrimination Investigation Unit. The agency coordinator will complete the complaint intake report and obtain a completed copy of the complaint form from the employee filing the complaint. The coordinator will forward a copy of the completed intake report to the agency's legal counsel and the Sexual Harassment/Discrimination Investigation Unit, along with any supporting documentation. The agency coordinator may also submit the complaint via NEATS.

2. The investigator will begin the investigation as soon as witnesses are available.

3. Investigations will be conducted as discreetly and with as little disruption to the workplace as possible. All information gathered in an investigation will be kept confidential, and

the confidential nature of the investigative process will be conveyed to the complainant, the accused and each witness.

4. The investigator will prepare a written report of findings, which will be submitted to the appointing authority, the agency's legal counsel, and the agency's chief personnel officer. The ultimate decision for remedial action is the responsibility of the appointing authority; however, the investigative staff may suggest mediation services, if appropriate.

5. After the investigation has been completed, the appointing authority will review the findings and recommendations and determine the appropriate resolution of the case. If warranted, the agency, after consultation with their legal counsel, may take disciplinary action up to and including termination. The agency shall retain a written record of the findings of the investigation and the resolution of the complaint as confidential records.

6. At the conclusion of the Division of Human Resource Management's Sexual Harassment/Discrimination Investigation Unit's investigation, the Division of Human Resource Management will notify the complainant in writing that the investigation was completed and forwarded to their agency for review. The agency, in consultation with their assigned legal counsel, shall notify both the complainant and the accused in writing at the conclusion of their administrative review. A copy of the Notification letter that is sent to the complainant and/or accused must be sent to the Sexual Harassment/Discrimination Investigation Unit for its files. Additionally, the agency shall take whatever corrective action it deems appropriate following consultation with its legal counsel. Corrective action that involves discipline of the accused is confidential pursuant to NAC 284.718 and must not be disclosed except as authorized pursuant to NAC 284.726.

C. Complaint Submitted Through the Hotline

1. When an employee transmits a complaint of sexual harassment or discrimination through the State hotline, the Sexual Harassment/Discrimination Investigation Unit will complete the initial intake report and/or submit the complaint in NEATS.

2. The agency coordinator will be notified of the complaint via NEATS.

3. The investigation will then proceed as described for complaints submitted to appointing authorities (*see* Item VI-B).

	**STATE OF NEVADA** **EXECUTIVE BRANCH** **SEXUAL HARASSMENT & DISCRIMINATION POLICY**

SEXUAL HARASSMENT AND DISCRIMINATION POLICY ACKNOWLEDGEMENT

EMPLOYEE NAME: _____

EMPLOYEE ID #: _____

DEPT/DIV/AGENCY/ORG #: _____

☐ I have read and understand the *Sexual Harassment and Discrimination Policy* dated 4/18/18.

EMPLOYEE SIGNATURE: _____

DATE: _____

SUPERVISOR SIGNATURE: _____

DATE: _____

STATE OF NEVADA

INFORMATION SECURITY PROGRAM POLICY
100 REV C

Original Publication Date: **October 28, 2008 Interim Approval**
Revision Date: March 30, 2017 Approval

Established and Approved by the:
Nevada State Information Security Committee

Approved by the:
State Chief Information Officer

Sponsored by the:
Enterprise IT Services
Office of Information Security

THIS PAGE INTENTIONALLY LEFT BLANK

Preface

Enterprise IT Services (EITS) has the statutory responsibility for establishing regulations and providing guidance to state entities 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, EITS 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 entities in establishing entity specific security policies, standards, processes and plans. NRS 242.101.

To ensure the security concerns and needs of state entities 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 entities 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 evolves, this document 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; and/or*
- *Legislative Audit findings that stem from security audit.*

The International Standard ISO/IEC 27002:2005 (E) Code of Practice for Information Security Management and the National Institute of Standards and Technology, NIST Publication 800 series were used as guidance in the development of this policy. All reference documents provide the best industry practices and the requirements of the federal government, which require state compliance due to receiving federal funds for information systems or from accessing, processing, storing or transmitting federal data.[The requirements of NIST 800-53 and 800-100 will be the de facto state standard in situations where neither the state nor the agency has established a policy or standard on a specific security control]

This policy has been developed and approved by the State Information Security Committee 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, 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 entities 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 entities within the Executive Branch of Nevada State Government, with the exception of the Nevada System of Higher Education and the Nevada Criminal Justice Information Computer System, comply with the direction of this policy.*

In cases where a state entity 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 EITS, 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.

Document Change History

Version Number	Release Date	Summary of Changes	Chapter Number/ Paragraph Number	Changes Made By
A	10/28/2008	Initial Document Release		
B	07/12/2011	Revised background checks.	3.4.2	S. Ingersoll
C	03/30/2017	Review and Update – Rename 4.100000	Multiple	EITS/OIS

TITLE	SIGNATURE	DATE
State IT Security Committee Chair State Chief Information Security Officer		
State Chief Information Officer		

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION

1.0 Purpose

The purpose of this policy is to define a set of minimum security requirements to protect state data and information technology (IT) systems that all state entities within the Executive Branch of Nevada State Government must meet. Any state entity, 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 entity IT systems;
- communicate the responsibilities for the protection of state entity information;
- establish a secure processing base and a stable processing environment within state entities and throughout the state;
- reduce to the extent possible the opportunity for errors to be entered into an IT system supporting a state entity business processes;
- preserve management's options in the event of state data, information or technology being misused, lost or unauthorized access; and
- promote and increase the awareness of information security in all state entities and with all state employees.

1.1 Scope and Applicability

This State Information Security Program Policy provides a baseline of security policies for the State of Nevada. This policy establishes mandatory policies to ensure confidentiality, integrity, availability, reliability, and non-repudiation within the State's infrastructure and its operations.

This policy applies to all state entities within the Executive Branch of Nevada State Government, excluding the Nevada System of Higher Education and the Nevada Criminal Justice Information Computer System, that operate, manage or use IT capabilities in support of the business needs of the entity. This policy is applicable to state employees, contractors and all other authorized users, including outsourced third parties, which have access to or manage state information. Where conflicts exist between this policy, a state entity policy or a federal policy, the more restrictive policy will take precedence.

This policy encompasses all systems for which the state has administrative responsibility, including systems managed or hosted by third parties on behalf of a state entity. It addresses all information, regardless of the form or format, which is created or used in support of business activities of state entities.

1.2 Authority

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 State Information Security Program Policy is the first step to ensuring compliance with these requirements.

Nevada Revised Statute (NRS) 242.101
The Clinger-Cohen Act of 1996
OMB Circular A-130, Management of Federal Information Resources and associated NIST Publications:
NIST 800-53 – Recommended Security Controls for Federal Information Systems and Organizations
NIST 800-100 – Information Security Handbook – Guide for Managers
Federal Information Security Management Act of 2002

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 2 OVERVIEW

This chapter provides an overview of this State Information Security Program Policy. It highlights the State's information security policy requirements, security responsibilities and summarizes subsequent sections of this document.

Enterprise IT Services (EITS) is responsible for establishing a State-wide information security program to assure that each information system and associated facility provides a level of security that is commensurate with the risk and magnitude of the harm that could result from loss, misuse, disclosure, or modification of the information contained in the system. Each system's level of security must protect the confidentiality, integrity and availability of the information and comply with all security and privacy-related laws and regulations.

The EITS Office of Information Security (OIS) must develop and administer the State Information Security Program that meets statutory, regulatory and State requirements, as well as the needs of the public. State entity Information Security Programs must comply with the State Information Security Program Policy and must meet the minimum standards set forth by this policy.

2.1 Document Organization

Security controls are delineated in three primary categories of administration, operational and technical, which is the organizational structure of this document. Best practices from the International Standard, ISO/IEC 27002:2005 (E), Code of Practice for Information Security Management and the National Institute of Standards and Technology, NIST Special Publication 800-100, Information Security Handbook, A Guide for Managers have been referenced and used to develop the State Information Security Program Policy.

- Chapter 3, **Security Administration** policies, focuses on security administration, risk assessment/management, asset management, personnel security, security awareness training, and security plans.

- Chapter 4, **Operational Policies**, focuses on security methods for physical security, environmental security, media control, data integrity, equipment security, security incident management.

- Chapter 5, **Technical Policies**, focuses on security controls that the computer executes including identification/authentication, system/data access control, audit trails, network security, encryption, and patch management

This document contains policies that satisfy minimum security requirements based on industry best practices and federal guidelines.

2.2 Document Change Control

Requests for changes to this policy must be presented by the state entity to Enterprise IT Services, Office of Information Security. The requested change will be formally drafted and submitted to the State Information Security Committee for review and approval. Once approved by the committee, the CISO will submit the change through the State Chief Information Officer (CIO) for final approval. Once final approval is granted, the CISO will cause the change to occur in this document and distribute the change to all state entities. It is the state entity's responsibility to communicate the approved changes to their organization.

2.3 Roles and Responsibilities

2.3.1 Enterprise IT Services (EITS), Office of Information Security (OIS) has the responsibility to:

A. establish, implement, administer and oversee the State Information Security Program;
B. develop guidance documents for state entities in developing various information security programs and plans;
C. provide subject matter expertise and assistance to state entities in establishing specific information security programs, development of information security policies, standards, procedures, and plans, information security awareness training, information security risk, vulnerability and physical security assessments;
D. establish a state Information Security Incident Management program to assist state entities in the determination if a security breach or incident has actually occurred and to provide an initial administrative review of the incident;
E. chair the State Information Security Committee and provide direction and guidance to the committee in the development of the State Information Security Program, policies and standards;
F. coordinate and obtain approval of all information security policies and standards from the State Information Security Committee and the State Chief Information Officer;
G. publish all approved information security policies, standards and procedures;
H. ensure that the state security policies and standards are reviewed and revised every two years.

2.3.2 State Agencies have the responsibility to:

A. establish and implement a departmental security program, to include policies, standards and procedures, that is consistent with or exceeds the requirements of this policy and commensurate with the risk and magnitude of harm of state information resources should unauthorized access, use, disclosure, disruption, modification or destruction occur;
B. ensure information security management processes are integrated with the state entities strategic and operational planning processes;
C. appoint an Information Security Officer (ISO) for the agency that will establish, administer, implement and oversee an agency Information Security Program;
D. communicate state and agency security policies, standards and procedures to all agency staff.

2.3.3 State agency Information Security Officers have the responsibility to:

A. ensure the establishment, implementation, enhancement, monitoring and enforcement of the federal, state and entity information security policies and standards;
B. provide direction and leadership to his or her management and staff through the recommendation of security policies, standards, procedures, processes and awareness programs to ensure that appropriate safeguards are implemented;
C. facilitate compliance with state and agency policies, standards and procedures;
D. represent the agency on the State Information Security Committee.

2.4 Exceptions to State Policies or Standards

A. In cases where a state agency cannot comply with any section of the State Information Security Program 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 EITS, Office of Information Security, Chief Information Security Officer (CISO) for approval.

B. Resulting risks from a deviation to policy must be documented in the appropriate Information Security Plan.

C. OIS will provide an overview of the exception list to the committee on an annual basis.

2.5 Compliance

2.5.1 EITS, Office of Information Security (OIS):

A. has oversight responsibilities to state agencies within the Executive Branch of Nevada State Government. The oversight is to provide a means to review and identify potential new or unaddressed vulnerabilities and to establish a baseline of a state agency and overall statewide security posture to build on to improve the overall security structure;

B. does not have enforcement authority of state security policies and standards; however, OIS has the responsibility to escalate unaddressed security vulnerabilities as the Chief Information Security Officer (CISO) deems necessary to the State Chief Information Officer (CIO) for resolution per NRS 242.

C. within the oversight responsibilities, may initiate security assessments of a state agency to identify new or unaddressed risks, threats, vulnerabilities of the State's information processing environments and infrastructures;

D. must provide the state agency with a written report of an assessment;

E. can only release the results of an assessment to other compliance or audit organizations upon written approval of the assessed state agency.

2.5.2 State Agencies must:

A. periodically review implemented security controls to verify compliance with state and agency security policies, standards, procedures and processes;

B. establish enforcement and consequences for state and agency security controls.

2.6 References

Policies provided in this document are based on industry standards and guidelines provided by:

- International Standard ISO/IEC 27002:2005 (E) – Code of Practice for Information Security Management
- National Institute of Standards and Technology (NIST) – 800 Series
- OMB Circular 130 – Management of Federal Information Resources

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 3: SECURITY ADMINISTRATION POLICIES

This State Information Security Policy is a statement that sets the direction, gives broad guidance and defines the minimum requirements, ethics, responsibilities and accepted behaviors required to establish and maintain a secure environment, and achieve State information security objectives. Compliance with this policy is mandatory. Exception requests can be submitted requesting an exception to a specific policy stated within this document but must be approved by the State Chief Information Security Officer (CISO).

3.1 Organizational and Functional Responsibilities

3.1.1 State Agencies:

A. Establish a framework to initiate and control the implementation of information security within their area of authority.

B. Appoint an Information Security Officer (ISO) for the state agency. The appointment may be based on the size of an agency, with individual ISO's appointed for each sub-organization within the agency, if the agency is large. The agency may also choose one ISO to represent and fulfill the ISO responsibilities for an entire agency or to serve as the agency's lead ISO, to coordinate with all agency ISOs on behalf of the agency.

C. Establish a process to determine information sensitivity, based on best practices, State directives, legal and regulatory requirements and identified security risks and vulnerabilities to determine the appropriate level of protection for the information and the operational environment of the agency.

D. Ensure the agency structure is in place for the:

1) establishment and implementation of agency specific information security program to include policies, standards and procedures;

2) assigning information security responsibilities;

3) implementation of a security awareness program;

4) monitoring significant changes in the exposure of information assets to major threats, legal or regulatory requirements;

5) coordination of security incidents with EITS, Office of Information Security;

6) consideration and planning of major initiatives to enhance information security within the agency;

7) ensure information security is included in the design of all automated applications;

8) communicating requirements of this policy and associated agency specific information security policies and standards to third parties and addressing third party agreements.

3.1.2 State Agency Information Security Officer (ISO):

The state agency Information Security Officer (ISO) is responsible for the overall development, implementation, enhancement, monitoring and enforcement of the agency specific Information Security Program policies, standards and procedures.

The appointed state agency ISO is responsible for:

A. providing direction and leadership to the agency management and staff through the recommendation of security policies, standards, processes and security awareness programs to ensure that appropriate safeguards are communicated, implemented and to facilitate compliance with the state and agency specific information security controls;

B. report and coordinate with EITS, Office of Information Security, security breaches or investigations;

C. coordinate and oversee agency security program activities and reporting processes in support of this State Information Security Program Policy and other security initiatives.

3.1.3 Agency Management:

A. Agency management is responsible to support and provide resources needed to enhance and maintain a level of control consistent with the State and state agency Information Security Program Policies based on the level of identified risks.

B. Agency management has the following responsibilities in relation to the security of information:

1) ensure processes, policies and requirements are identified and implemented relative to security requirements defined by the agency's business;

2) ensure the proper controls of information are implemented for which the state agency business have assigned ownership responsibility based on the identified classification designation;

3) ensure the participation of the state agency ISO and technical staff in identifying and selecting appropriate and cost-effective security controls and procedures and in protecting information assets;

4) ensure participation of the state agency ISO in the development, selection and implementation of all Request for Proposals and Contracts involving information technology resources;

5) ensure appropriate security requirements for user access to automated information are defined for files, databases and physical devices assigned to their areas of responsibilities;

6) ensure critical data and recovery plans are backed up and kept at a secured off-site storage facility and that recovery of backed-up media will work if and when needed.

3.1.4 State Employees:

A. All state employees have the responsibility to protect state information and resources, including passwords, and to comply with the State and employee state agency Information Security Program Policies, Standards and Procedures.

B. All state employees must report suspected security incidents to the appropriate manager and to their agency's Information Security Officer (ISO).

3.2 Information Security Policy

3.2.1 General

A. All information, regardless of the form or format, which is created, acquired, stored or used in support of state agency's business activities, must only be used for official state business. State information is an asset and must be protected from its creation, through its useful life, and to its authorized disposal.

B. State information must be maintained in a secure, accurate and reliable manner and be readily available for authorized use.

C. State information/data must be classified and protected based on its importance to the business activities and risks to any given state agency.

D. Access to state information and information systems must be granted to an individual for only that information or systems required to accomplish the duties of their position.

3.2.2 Individual Accountability

Individual accountability is the cornerstone of any security program. Any person having authorized access to state information must:

A. be assigned unique user-id(s) and password(s) for access into state information systems. The original recipient of the user-id(s) and password(s) must not share their user id or password;

B. only use state information for official business;

C. only access IT systems and information for which they are authorized;

D. be responsible to reasonably protect against unauthorized activities performed under their user-id;

E. report suspected or actual security breaches or incidents, inappropriate content or system access/activity to the state entity's management and ISO or to the EITS, Office of Information Security.

3.2.3 Confidentiality – Integrity – Availability

All state entity information must be protected from unauthorized access to help ensure the information's confidentiality and maintain its integrity. State entities must:

A. classify and secure information within their jurisdiction based on the information's value, sensitivity to disclosure, consequences of loss or compromise and ease of recovery.

B. define appropriate processes and develop recovery plans and implement those processes to ensure the reasonable and timely recovery of all state entity information, applications, systems and security regardless of computing platform, should that information become corrupted, destroyed or unavailable for a defined period.

3.2.4 State Entity Security Program

A. State entities must approve, adopt, publish and communicate to all employees a statement on Information Security detailing management commitment and organizational approach to managing information security within the entity.

B. State entities must periodically review the statement at established intervals or when significant changes occur to update, reinforce and ensure the continued management commitment and approach for the entity's information security program.

3.3 Organizational Security Policy

3.3.1 Management Commitment to Information Security

A. Management must actively support security efforts within the entity through clear direction, demonstrated commitment, and explicit assignment of information security responsibilities to the entity ISO.

B. Information security initiatives and activities should be coordinated with representatives from different areas within the entity with relevant roles and job functions. All information security responsibilities should be clearly defined.

3.3.2 Information Security Function

The purpose and mission of the Information Security function is to:

A. develop, deploy and maintain an information security architecture that will provide security policies, mechanisms, processes, standards and procedures that meet current and future business needs of the state entity;

B. provide information security consulting to the state entity regarding security threats that could affect the entity's computing and business operations, and make recommendations to mitigate the risks associated with those threats;

C. assist management in the implementation of security measures that protect the IT infrastructure, while at the same time meet the business needs of the state entity;

D. develop and implement security training and awareness programs that educate employees, contractors and vendors with regard to the entity's information security requirements;

E. participate in the development, implementation, maintenance and testing of Continuity of Operations Plans (COOP), processes and techniques to ensure the continuity of the entity's business and security controls, in the event of an extended period of computing resource unavailability;

F. report to management and the EITS, Office of Information Security breaches of security controls, and implement additional compensating controls when necessary to help ensure security safeguards are maintained.

3.3.3 Role and Responsibility of the State Entity Information Security Officer

The state entity Information Security Officer (ISO) is responsible for performing, at a minimum, the following tasks;

A. develop or coordinate the development and implementation of state entity information security plans, policies, standards, procedures, and other control processes that meet the business needs of the state entity;

B. provide security consultation to the state entity management with regard to information security practices and controls;

C. work closely with entity management to ensure security measures are implemented to meet policy requirements;

D. evaluate new security threats and countermeasures that could affect the state entity and make appropriate recommendations to management of the state entity to mitigate the risks;

E. inform and coordinate reports of suspected information security incidents or breaches, unauthorized use and unauthorized disclosure of state information or personal identification information with state entity management and the EITS, Office of Information Security (OIS). OIS will provide support to all state entities suspecting a breach or incident by performing an initial administrative investigation of the associated IT resource(s), maintain the required chain of custody of all materials, equipment, and evidence and provide a neutral independent third party review and report to management to assist in making informed decisions on further actions;

F. ensure appropriate follow-up to security violations is conducted;

G. establish and provide appropriate security awareness and education to all state entity employees and where appropriate third party contractors;

H. be aware of laws and regulations that could affect the security controls and classification requirements of the state entity's information;

I. support, develop and accomplish actions required by the state entity ISO as defined in other parts of this State Information Security Program Policy;

J. represent the entity on the State Information Security Committee.

3.4 Personnel Security

3.4.1 General

The Personnel Security process begins with a review of the user's position needs, relevant policies, regulations, standards and threats for a defined environment.

A. All state entities must comply with existing state and federal laws, and regulations that impose significant responsibilities on employees for the security of information.

B. All state entities must establish an Acceptable Use Policy and obtain a signature from the employee indicating acknowledgement of the rules prior to access being granted to information or information systems.

3.4.2 Employment Screening

A. STATE EMPLOYEES and IT CONTRACTORS:

1) Fingerprint based background checks must be conducted on all persons hired, promoted or contracted for IT services determined to be sensitive. This requirement is supported by NRS 239B, Disclosure of Personal Information to Governmental Agencies.

2) Background checks must be processed through the Department of Public Safety and must consist of a State and a Federal Bureau of Investigation (FBI) fingerprint based background check. A conviction in any jurisdiction of any crime involving moral turpitude or indication of lack of business integrity or honesty, whether denominated a felony or misdemeanor, must be considered to be an unfavorable result of a background check. Any unfavorable results from a background check must be submitted to the State Chief Information Security Officer (CISO).

3) Unfavorable results from a background check must not be an automatic cause to refuse employment or cause for termination. The agency head after consult with the State Chief Information Security Officer (CISO) has the final decision on action to be taken or not taken based on the results of the report and disposition of court information.

3.4.3 Acceptable Use

A. Acceptable Use Policy must be developed for the entity's IT resources, including computers, telecommunications equipment, software and other data/information services. The policy must provide specific rules for the access and use of the entity's IT systems and information to include acceptable use of the Internet, e-mail, personal use of assigned IT systems, and use of mobile devices.

B. Each employee, contractor and vendor must sign and acknowledge receipt of the Acceptable Use Policy prior to granting access to entity IT systems or information, with annual review and acknowledgement.

3.4.4 Separation of Duties

Identified sensitive positions must have critical functions divided among different individuals, whenever possible, to ensure that no individual has all necessary authority or information access that could result in fraudulent activities and misuse of confidential/privileged information.

3.4.5 Resignation/Termination

A. A process must be developed to establish, implement and maintain procedures for processing terminations, both voluntary and involuntary, of employees. The procedures for processing termination involving sensitive positions or access to sensitive information must be more restrictive than those in non-sensitive positions.

B. Involuntary termination of an employee must cause immediate revocation of all system and information access privileges.

3.5 Security Awareness

3.5.1 On-going awareness training programs that addresses the security education needs of all state entity employees must be developed and provided.

3.5.2 Security awareness training must be developed by the State entity Information Security Officer to supplement the entity's new employee orientation program and must be reinforced at least annually with all entity employees.

3.6 Asset Management

3.6.1 State entities must establish and maintain protection of their information technology assets.

3.6.2 An inventory of assets must be maintained by state entities. The asset inventory must include:

A. Physical assets: computer equipment, communications equipment, removable media and other equipment;

B. Software assets: application software, system software, development tools, and utilities;

C. Information: entity-defined essential data, system documentation, operational and support procedures; information security plans, contingency and continuity of operations plans.

3.6.3 Updated inventories must be included in the appropriate Information Security and Contingency Plans.

3.7 Risk Assessment and Risk Management

Risk Assessments are the foundation to establish an effective and appropriate Information Security Program to define and establish necessary controls and processes, commensurate with the level of risks, necessary to provide protection to a state entity's information processing infrastructure and information.

3.7.1 Risk Assessments

A. A full risk assessment must be conducted at each state entity to determine the risks, threats, and vulnerabilities to their IT systems, applications, information and operational controls and processes. The full risk assessment must include:

1) **security administration assessment** of information security controls, policies, standards, procedures and processes, data classification, information security plans;

2) **vulnerability assessments** of IT systems and applications, to include networks, servers, wireless, web sites, e-mail systems, data access controls;

3) **physical security assessments** of entity offices for physical access and environmental controls.

B. Initial risk assessments must be conducted by an independent party with expertise in information security and specific technical expertise.

C. Results of the assessments must be used to determine the level of protection to be provided and to develop, administer, implement and maintain the state entity Information Security Program which must consist of entity specific security policies, standards, procedures, processes, internal controls and continuity of operation plans.

D. The appropriate assessment must be conducted prior to the introduction of a new system applications or when a major change occurs to the operating environment.

3.7.2 Self-Assessments

State entities must conduct a self-assessment of their information security controls at least annually and revise their controls according to identified inadequacies or new risks.

3.7.3 Independent Review of State Entity Information Security Program

State entities must have a periodic independent review of established security controls. The Enterprise IT Services (EITS), Office of Information Security (OIS) should be the first resource considered for the independent reviews.

3.8 Information Security Plans

Each state entity must develop Information Security Plans to document the administrative security controls and the controls for each major application and general support systems.

3.8.1 Administrative Security Plan

A. Each state entity must develop and document the administrative security controls established to include but not limited to controls put in place for security management, personnel security, security awareness training.

B. The Administrative Security Plan must be reviewed and revised at least biennially.

3.8.2 Major Application Security Plan

A major application is defined as an application that is critical to the business function of the state entity and/or requires special attention to security due to the risk and magnitude of impact to the state entity should the application be subject to unauthorized access, manipulation or disclosure of information.

A. Each state entity must develop and document the security controls designed within each major application of the entity. The plan must include the controls incorporated within the system design and any additional controls.

B. Major Application Security Plans must be developed prior to any new application being put into production.

C. Major Application Security Plans must be reviewed at least biennially or when a major change is made to the application.

3.8.3 Major Support System

A major support system is defined as an information system requiring special management attention because of its importance or criticality to the state entity's business and plays a significant role in the administration of the entity critical programs, finances, property or other critical resource.

A. Each state entity must develop and document the security controls designed within each major support system of the entity. The plan must include the controls incorporated within the system design and any additional controls.

B. Major Support System Security Plans must be developed prior to any new system being put into production.

C. Major Support Security Plans must be reviewed at least biennially or when a major change is made to the system.

3.8.4 General Support System Security Plan

General support systems are defined as one or a combination of multiple systems that support the state entity, such as a Local Area Network (LAN), Wide Area Network (WAN) or email server.

A. Each state entity must develop and document the security controls established for each general support system of the entity.

B. General Support System Security Plans must be developed prior to a new system is put into production.

C. General Support System Security Plans must be reviewed at least biennially or when a major change is made to the system.

3.9 Contingency Planning

State entities must implement and maintain a business continuity management process to minimize the impact on the organization, counteract interruptions to business activities and protect critical business processes from the effects of major failures of information systems.

3.9.1 Major Application Contingency Plan

A. State entities must develop a contingency plan for each major application that defines the backup and recovery procedures specific to each application.

B. Contingency plans must include all pertinent information required to identify any applications that the major application relies on to accomplish processing or any applications that the major application supplies data or processing capabilities to.

C. State entities must test the procedures defined in the application contingency plans at least biennially or when a major changed to the application has been implemented.

3.9.2 Major System Contingency Plan

A. State entities must develop a contingency plan for each major system that defines the backup and recovery procedures specific to each application.

B. Contingency plans must include all pertinent information required to identify any applications that the major system relies on to accomplish processing or any applications that the major application supplies data or processing capabilities to.

C. State entities must test the procedures defined in the application contingency plans at least biennially or when a major changed to the application has been implemented.

3.9.3 General Support System Contingency Plan

A. State entities must develop a contingency plan for each general support IT system that defines the backup and recovery procedures specific to each system.

B. Contingency plans must include all pertinent information required to identify all applications that resides on the general support system, operating system, users, datasets, and responsibilities for the backup and recovery of the system.

C. State entities must test the procedures defined in the general support system contingency plans at least biennially or when a major changed has been implemented.

CHAPTER 4: OPERATIONAL SECURITY POLICIES

4.1 Physical Security and Environmental Controls

4.1.1 Physical Access

Appropriate controls must be implemented to:

A. limit access to rooms, work areas/spaces and facilities that contain the entities information systems, networks and data to authorized personnel only;

B. deter, detect, monitor, restrict and regulate access to sensitive areas at all times;

C. ensure controls are commensurate with the level of risk and must be sufficient to safeguard the IT resources against possible theft, loss, destruction, accidental damage, hazardous conditions, fire, malicious actions and natural disaster.

4.1.2 Physical Security

Appropriate controls must be implemented to ensure that rooms, work areas/space and facilities that contain IT resources that process, transmit or store sensitive or privacy information are protected from unauthorized access.

4.1.3 Visitor Access

A. Controls must be implemented that restrict and control visitor access at all times to rooms, work areas/spaces and facilities that contain entity IT resources.

B. Visitor Logs must be established to record visitor access to work areas/spaces that contain sensitive IT equipment such as servers and communications equipment room.

4.1.4 Fire Protection

All systems and networks must be protected against the danger of water damage due to leakage from building plumbing lines, shut-off valves and other similar equipment through the location of equipment or covers for the equipment.

4.1.5 Supporting Utilities

A. An alternate power supply, such as a generator, must be installed to protect large critical IT systems from power spikes, brownouts, or outages.

B. State entity servers must be protected by an appropriately sized uninterruptible power supply.

C. Desktop computers supporting critical functions of a state entity must be protected by an uninterruptible power supply.

4.2. Equipment Security

4.2.1 Workstations

Appropriate controls must be implemented commensurate with the sensitivity level of the data accessed, processed or stored on the workstation.

4.2.2 Laptops and Other Mobile Computing Devices

Appropriate controls must be implemented to ensure that the storage and transmission of an entity's sensitive data is protected with encryption standards that are commensurate with the sensitivity level of the data.

4.2.3 Personally Owned Equipment and Software

A. State entities must control the use of personally owned or non-state equipment and software to process, access, or store state data. Personally owned or non-state equipment and software includes, but is not limited to, personal computers and related equipment and software, Internet service providers, personal e-mail providers (e.g., Yahoo, Hotmail), personal library resources, and handheld or personal digital assistant (PDA) devices.

B. Personally owned equipment and software must not be used to process, access, or store sensitive information or be connected the state enterprise or state entity's systems or network without the written authorization of the appropriate entity management and/or Information Security Officer.

4.2.4 Hardware Security

Hardware products must provide dependable, cost-effective security controls and features and preserve the integrity of the security features provided through the system software.

4.2.5 Hardware/Software Maintenance

A. Entity hardware and software must be tested, documented and approved prior to being placed into production.

B. Maintenance must only be provided by authorized personnel.

4.3 Media Control

Entities must establish procedures to protect media input/output data and system documentation from unauthorized disclosure, modification, removal and destruction.

4.3.1 Media Protection

Electronic media (e.g., disk drives, CDs, internal and external hard drives and portable devices) must be protected including backup media, removable media and media containing sensitive information from unauthorized access.

4.3.2 Media Marking

Media containing data must be marked and labeled to indicate the sensitivity level of the data.

4.3.3 Sanitization and Disposal of Information

Methods must be developed and documented to ensure that sanitization and disposal of media is commensurate with the sensitivity and criticality of the data residing on the storage devices, equipment and hardcopy.

4.3.4 Input/Output Controls

Physical, administrative and technical controls must be established and implemented to prevent unauthorized entry into office suites, operations, data storage, library and other restricted areas to restrict the unauthorized removal of media.

4.4 Data Integrity

State entities must establish formal procedures for backup, recovery and storage of data and related software.

4.4.1 Controls

Systems and networks must be equipped with data integrity and validation controls to provide assurance that information has not been altered.

4.4.2 Documentation

Documentation for all systems, networks, and applications must be developed, readily available to appropriate personnel, secured and up to date for routine security audits, tests and unexpected events such as system disruptions, failures or outages.

4.5 Configuration Management

4.5.1 Controls must be established, implemented and enforced on all state entity systems and networks that process, store, or communicate sensitive information.

4.5.2 Controls must include processes for the request, approval, implementation and documentation of all configuration changes.

4.6 Software Security

State entities must establish controls to ensure that only state approved and properly licensed software is installed on state systems.

4.7 Software Development and Maintenance

4.7.1 Separate development, test and production environments must be established on state systems.

4.7.2 Processes must be documented and implemented to control the transfer of software from a development environment to a production environment.

4.7.3 Development software and tools must be maintained on computer systems isolated from a production environment.

4.7.4 Access to compliers, editors and other system utilities must be removed from production systems.

4.7.5 Controls must be established to issue short-term access to development staff to correct problems with production systems allowing only necessary access.

4.7.6 Security requirements and controls must be identified, incorporated in and verified through out the planning, development, testing phases of all software development projects. Security staff must be included in all phases of the System Development Lifecycle (SDLC) from the requirement definition phase through implementation phase

4.7.7 Vulnerability testing must be conducted on all systems prior to being placed into production.

4.8 Security Incident Management

4.8.1 State entities must establish and maintain an incident response capability to include preparation, identification, containment, eradication, recovery and follow-up capabilities to ensure effective recovery from incidents.

4.8.2 State entities must adhere to a standard methodology for resolving information security events to ensure a consistent and effective method is applied.

4.8.3 A process of evaluation and continual improvement must be applied to information security events after completion.

4.8.4 Individual must report any observed or suspected information security events or weaknesses to their manager or entity Information Security Officer.

4.8.5 A formal report must be developed following the discovery of an event or weakness, to allow for timely corrective action.

4.8.6 A security incident involving the disclosure of personal identifiable information (PII) must follow the notification rules of NRS 603A.220, Disclosure of Breach of Security of System Data, Methods of Disclosure.

4.8.7 State entities must promptly notify the EITS, Office of Information Security of a suspected or actual disclosure of Personal Identifiable Information. The EITS, OIS must be included in the investigation and corrective actions.

CHAPTER 5: TECHNICAL SECURITY POLICIES

5.1 Identification and Authentication

Users of state IT systems and networks must be individually identified and accountable for all actions on those systems accessed by that identification

5.1.1 Identification

Each authorized user of state systems and networks must have a unique UserID.

5.1.2 Password

A. Logical password controls must be used in conjunction with a unique UserID.

B. Each authorized user of state systems and networks must have a unique password that is to remain confidential, not to be shared with other users, system maintenance personnel and/or contractors.

C. Passwords granting access to sensitive data or elevated access to the system must not be saved, stored or hard-coded in any system or application.

5.2 Data Access Controls

State IT systems and networks must have logical access controls to provide protection from unauthorized access, alteration, loss, disclosure and availability of information.

5.2.1 Review and Validation of System User Accounts

User accounts must be reviewed quarterly to ensure the continued need for access to a system and that transferred or resigned users have been deleted.

5.2.2 Automatic Account Lockout

State IT systems and networks must have automatic account lockout after a third failed attempt to log-in to the system or network.

5.2.3 Automatic Session Timeout

State IT systems must have automatic session timeout and re-authentication to re-establish or unlock. The timeout setting will be determined by the entity ISO consistent with the sensitivity of the data and security of the work area.

5.2.4 Warning Banner

State IT systems and network must display an entity or State Attorney Generals' Office approved sign-on warning banner at all system access points.

5.3 Audit Trails

5.3.1 All IT systems and networks must generate audit logs that show addition, modification and/or deletion of information.

5.3.2 Audit logs must be recorded, retained and regularly analyzed to identify unauthorized activity.

5.4 Network Security

5.4.1 Network Management

Network infrastructure must be managed and controlled to protect systems and applications using the network including information in transit.

5.4.2 Remote Access and Dial-In

Remote access and dial-in security controls must be implemented and enforced to provide protection for information stored, accessed, transmitted and received across public and private networks.

5.4.3 Network Security Monitoring

All state systems and networks must have security event-monitoring.

5.4.4 Firewalls

All incoming and outgoing connections from state systems and networks to the Internet and extranets must always be made through a firewall.

5.4.5 Internet Security

Connectivity of state systems and networks to the Internet must be within a framework of effective technical security controls using firewalls and gateways that provide external network access via Internet Service Providers (ISP) and other public or designated external entities.

5.4.6 E-Mail Security

A. State e-mail services must have security controls implemented to protect against malicious code attacks and ensure that e-mail services are not used to relay unauthorized messages.

B. State e-mail services must be used for only official state business.

5.4.7 Personal E-Mail Accounts

Personal e-mail accounts must not be accessed using state systems and networks without the entity management approval.

5.4.8 Security Testing and Vulnerability Assessment

All state systems and networks must have vulnerability scans and/or penetration tests to identify security threats prior to the initiation of a new system or network and at least annually for existing systems or networks.

5.5 Malicious Code Protection

All state systems and networks must have protection programs to minimize the risk of intruding malicious code (e.g., viruses, worms, Trojan horses).

5. 6 System-to-System Interconnection

Each state entity must implement a plan or schedule to establish, maintain and terminate interconnections among state entity systems and networks that are operated by different state or federal organization.

5. 7 Patch Management

State entities must establish and implement patch management to all systems and networks in a manner that ensures maximum protection against security vulnerabilities and minimize impact on entity business operations.

Patch management must contain a systematic process of identifying, prioritizing, acquiring, implementing, testing and validating security patches necessary for each system or network.

A risk-based decision must be documented if security patches are not applied to a system or network.

5.8 Communications Security

5.8.1 Voice Communications

Security controls must be implemented to provide adequate protection at the system and environmental levels.

5.8.2 Data Communications

Controls must be established to ensure that sensitive data is protected from unauthorized access during transmission.

5.8.3 Wireless Communications

A. Wireless networks must not be connected to wired networks except through appropriate controls (e.g., Virtual Private Network (VPN) port).

B. Wireless LANS must not be used to transmit, process, or store sensitive information unless protected with encryption standards that are commensurate with the sensitivity level of the data.

5.8.4 Peer-to-Peer File Sharing

Peer-to-Peer file sharing must only be permitted internally between state entities.

5.8.5 Instant Messaging

Instant messaging is only permitted internal to state systems and networks.

5.8.6 Video Conferencing

Adequate controls must be implemented to ensure that appropriate transmission protections are in place commensurate with the highest sensitivity of the information to be discussed over the video conference.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

REQUIREMENTS AND PROCEDURE FOR REQUESTING EXCEPTION

TO STATE INFORMATION SECURITY POLICIES AND STANDARDS

Requirements and Procedure for Exception Requests

1.0 PURPOSE

State information security policies and standards provide guidance for the security and effective planning and use of information technology (IT) resources. In the diverse State IT infrastructure, there may be occasions when compliance with a policy or standard cannot be accomplished; justifications for the noncompliance must be documented.

This policy establishes a mechanism to address requests for an exception to State Information Security policies or standards.

1.1 REQUIREMENTS

1.1.1 State entities that are unable to comply with a State Information Security Policy or Standard must formally request an exception when there is a legitimate reason and reasonable alternatives to meet the policy or standard are not viable.

1.1.2 Exceptions will be evaluated and granted on a case by case basis and consider the nature of the request, systems impacted, security risks, and mitigation alternatives.

1.1.3 Request for exception must be submitted by the appropriate state entity manager, IT manager, Information Security Officer (ISO) or their designee.

1.1.4 Requests must be submitted utilizing the formalized exception request process defined in this document.

1.1.5 Request for an exception must be submitted to the Enterprise IT Services (EITS), Office of Information Security (OIS) for review. OIS will provide the requestor with written notification of the results of any exception request.

1.1.6 Exception requests that are denied by the OIS, Chief Information Security Officer (CISO) may be appealed to the State Chief Information Officer (CIO).

1.1.7 Approved exception requests must be kept on file for audit purposes.

1.1.8 All exceptions requests are temporary and must be reviewed annually.

1.2 PROCEDURE

1.2.1 A request for exception must use the Exception Request Form. The exception request must include the following:

A. the number and title of the policy or standard the exception request is covering;

B. the business and technical reasons for the exception – requests without specific business or technical reasons identified in the justification will be denied and returned for resubmission;

C. the source and destination addresses and specific ports that require exception if applicable;

D. the specific, temporary length of time the exception will be required;

E. the actions that will be taken to eliminate the exception;

F. the timeframe to eliminate the exception.

1.2.2 The Exception Request Form must be submitted to OIS and assigned to an OIS staff member for review. The request will be evaluated and presented with comments and a recommendation to the CISO for review.

1.2.3 The CISO must evaluate the request, consider the OIS staff recommendation, and grant or deny the request as appropriate. The assigned OIS staff will notify the requestor via e-mail of the decision.

1.2.4 The assigned OIS staff will provide a copy of the final decision to the requestor via inter-departmental mail.

1.2.5 OIS will maintain a copy of all Exception Requests with decision on file.

1.2.6 Granted exception requests will be reviewed annually, in January, by OIS.

1.2.7 The decision of the CISO related to this procedure may be appealed to the CIO. The process to appeal the CISO decision is:

A. Send the original exception request forms with a memo to the CISO directly, stating the reason(s) why the exception should be approved from the state entity's perspective.

B. The CISO will re-evaluate the exception and submit it to the EITS senior security team (e.g., consist of the CIO, CISO and Deputy CISO) for final decision.

C. The CISO will return the decision of the EITS senior security team to the requestor.

NEVADA STATE BOARD OF PHARMACY
IT ACCEPTABLE USE AGREEMENT

INTRODUCTION

This acceptable use agreement governs the use of computers and mobile devices, networks, and other information technology (IT) resources for the Nevada State Board of Pharmacy (Board). This statement applies to all Board members, employees and contractors, and all other persons who may legally or illegally use or attempt to use IT resources owned or managed by the State, and/or is connected by any means to the state SilverNet Network. As a user of these IT resources, you are responsible for reading and understanding this agreement.

IT resources at the Board are to be used in a manner that supports the mission of the Board. IT resources refer to all equipment, hardware, software or network (including wireless networks) and includes computers and mobile devices, e-mail applications and state internet and intranet access (including when accessed through personally owned computers). IT resources range from multi-user systems to single-user terminals and personal computers, whether free-standing or connected to networks.

ACCEPTABLE/UNACCEPTABLE USE

1. All users must safeguard the confidentiality, integrity, and availability of Board IT resources, including password login, access codes, network access information and log-on IDs from improper access, alteration, destruction, or disclosure. Users shall only access or use Board IT resources when authorized. Users must abide by Board policies and other State policies regarding the protection of data and information stored on these IT resources.

2. When personally-owned IT resources are used for Board business, the Board retains the right to any Board records or materials developed for Board use. Also, any materials must be appropriately safeguarded according to applicable standards including, but not limited to, virus protection, protected access and backups.

3. Users must not use Board IT resources to engage in activities that are unlawful or violate federal or state laws, State or Board security policies or in ways that would:
   a. Be disruptive, cause offense to others, or harm morale.
   b. Be considered harassing or discriminatory or create a hostile work environment.
   c. Result in State or Board liability, embarrassment, or loss of reputation.

4. Users must maintain the integrity of information and data stored on Board IT resources by:
   a. Only introducing data that serves a legitimate business purpose.
   b. Only acquiring, using, altering, disposing of, or destroying data or information with proper authorization.
   c. Protecting data and information stored on or communicated across Board systems and accessing appropriate data or information only when authorized.
   d. Protecting data and information communicated over internal or public networks to avoid compromising or disclosing nonpublic information or communications.

5. While Board IT resources are primarily intended for business purposes, limited (incidental and occasional) personal use may be permissible when authorized by management and it does not:
   a. Interfere with work responsibilities or business operations.
   b. Involve interests in personal outside business or other non-authorized organizations or

activities (which may include, but are not limited to, selling personal property, soliciting for or promoting commercial ventures, or soliciting for or promoting charitable, religious, or political activities or causes).

c. Violate any of the federal or state laws or State or Board security policies.
d. Lead to inappropriate cost to Board functional units. Excessive non-work-related surfing and utilizing streaming services such as listening to music or watching videos is prohibited.
e. External Internet based instant messaging is forbidden.
f. Peer-to-peer file sharing is specifically forbidden.

6. Users must check all electronic media, such as software, diskettes, CDs and files for viruses when acquired through public networks (e.g., internet sites) or from outside parties by using virus detection programs prior to installation or use. If users suspect a virus, the applicable system(s) or equipment must not be used until the virus is removed. The matter must be immediately reported to the applicable manager or the Board (ISO).

7. Only Board-approved and properly licensed software will be used or installed on Board computers and mobile devices and will be used according to the applicable software license agreements. Security awareness training must be reinforced annually for all users of State information and information technology.

8. Users must ensure that any nonpublic information, data or software that is stored, copied, or otherwise used on Board IT resources is treated according to the State and Board standards regarding nonpublic information and applicable agreements and intellectual property restrictions.

9. Whenever a user ceases to be an employee, contractor, or other authorized user of Board IT resources, such user shall not use Board facilities, accounts, access codes, privileges, or information for which he/she is no longer authorized. This includes the return of all Board IT resources including hardware, software, data, and peripherals.

10. Inappropriate use of e-mail includes, but is not limited to, sending and forwarding:
    a. Messages, including jokes or language, that may be considered discriminatory, harassing, unlawful, defamatory, obscene, offensive, insensitive, or otherwise inappropriate (for example, messages about age, race, gender, disability, sexual orientation, national origin or similar matters).
    b. Pornographic or sexually explicit materials.
    c. Chain letters.
    d. Information related to religious materials, activities, or causes, including inspirational messages.
    e. Charitable solicitations unless sanctioned by the State or Chief Information Officer (CIO).
    f. Auction-related information or materials unless sanctioned by the State or CIO.
    g. Software or copyrighted materials without a legitimate business or instructional purpose.
    h. Large personal files containing graphics or audio files (such as photographs and music).
    i. Materials related to personal commercial ventures or solicitations for personal gain.
    j. Information related to political materials, activities, or causes unless sanctioned or permitted by the State or CIO.
    k. Unauthorized or inappropriate mass distribution or communication.

l. Any other materials that would be improper under this policy or other State or Board policy.

11. Inappropriate use of the internet includes, but is not limited to, accessing, sending, or forwarding information about, or downloading from:
    a. Sexually explicit, harassing, or pornographic sites.
    b. “Hate sites” or sites that can be considered offensive or insensitive.
    c. Auction or gambling sites.
    d. Games, software, audio, video, or other materials that the Board is not licensed or legally permitted to use or transmit, or that are inappropriate or not required by State or Board business.
    e. Offensive or insensitive materials, such as sexually or racially oriented topics.
    f. Any other materials that would be improper under other State or Board policies.
    g. Intentional importation of viruses, keyloggers, Trojans, or any other software that could be classified as malware or spyware.

CONSEQUENCES

Any inappropriate use of Board IT resources may be grounds for discipline up to and including dismissal. Should disciplinary action be required, the State of Nevada, progressive disciplinary procedures will be followed.

NEVADA STATE BOARD OF PHARMACY

ACCEPTABLE USE AGREEMENT
ACKNOWLEDGEMENT

This is to certify that I have read and agree to abide by the guidelines set forth within the Board Acceptable Use Agreement. As a member, employee or contractor of the Board, I fully intend to comply with this policy realizing that I am personally liable for intentional misuse or abuse of the Board's IT resources. If I have any questions about this policy, I understand that I need to ask the Executive Director or his/her authorized agent for clarification.

**If I refuse to sign this acknowledgement form, the Executive Director or his/her authorized agent will be asked to sign this form indicating that I have been given time to read and have had questions answered about this agreement. The Executive Director or his/her authorized agent will read this statement to me prior to signing the document and advise me that by not signing this document my rights to use the Board's IT resources may be denied and may affect my ability to fulfill my duties.*

NAME (please print)	
SIGNATURE	
TITLE/POSITION	
DATE	

---

*EXECUTIVE SECRETARY'S SIGNATURE	
COMMENTS	
DATE OF NEXT REVIEW AND AGREEMENT	

Date of next review should coincide with date of next Performance Evaluation, contract renewal, or re-appointment to the Board, as applicable.

Nevada Executive Branch Employees
Acknowledgment of Ethical Standards

Employee Information

Name:		**Employee ID #:**	
Department:		**Agency #:** (3 digit, e.g. 070)	
Division:		**Home Org. #:** (4 digit, e.g. 1363)	
Date Hired:		**Class Code:**	

NRS 281A.500(2) requires that each new public employee receive information regarding Nevada Ethical Standards. The Nevada Ethics In Government Manual and a link to NRS 281A can be located on the Nevada Commission on Ethics website at the following: http://ethics.nv.gov or on the Division of Human Resource Management's website at: http://hr.nv.gov/Resources/Forms/Ethics/Ethics/.

By signing this form, I acknowledge that I have been provided information on Ethics as required by NRS 281A.500(2) and I acknowledge that I must familiarize myself with the Ethics in Government laws as they pertain to my conduct as a public employee.

Signature: _____ **Date:** _____

Distribution: **Original - Division of Human Resource Management, Central Records**
Copy – Employee
Copy – Agency file

Note: Form must be completed within 30 days of new hire date.

NEVADA STATE BOARD OF PHARMACY
POLICY FOR SCREENING OF STAFF TO AVOID CONFLICTS OF INTEREST

These policies and procedures are implemented pursuant to NRS 622.210 and the Nevada Ethics in Government Law, NRS Chapter 281A.

All employees of the Nevada State Board of Pharmacy (Board) shall consent to these policies and procedures as a condition of employment; evidence of such consent shall be made by execution of a copy of these policies and procedures below.

Board employees have a duty to carry out and enforce the provisions of Nevada law to protect the health, safety and welfare of the public. *See* NRS 622.080, NRS 639.070(1)(a), NRS 639.213 and NRS 639.2171(1).

NRS 281A.020(1) provides:

> It is hereby declared to be the public policy of this State that:
>
> (a) A public office is a public trust and shall be held for the sole benefit of the people.
>
> (b) A public officer or employee must commit himself or herself to avoid conflicts between the private interests of the public officer or employee and those of the general public whom the public officer or employee serves.

Board employees have a duty to avoid any real or perceived conflict of interest in any transaction or matter over which the Board has supervision, control, jurisdiction or advisory power. *See* NRS 281A.400 - .430.

In any transaction or matter in which the Executive Secretary has a real or perceived conflict of interest, including, without limitation, any transaction or matter involving an immediate relative as defined in NRS 622.020, upon discovery of the conflict the Executive Secretary shall immediately recuse him/herself from participating in the transaction or matter, including by refraining from attempting to influence any deliberation or action on the transaction or matter, and not be privy to any non-public information relating to the transaction or matter. In the event of such a recusal, the Deputy Executive Secretary shall have exclusive management authority over the transaction or matter and shall take all necessary action to sequester the Executive Secretary from the transaction or matter, subject only to the oversight of the Board.

In any transaction or matter in which any Board employee other than the Executive Secretary has a real or perceived conflict of interest, including, without limitation, any transaction or matter involving an immediate relative as defined in NRS 622.020, upon discovery of the conflict the employee shall immediately recuse him/herself from participating in the transaction or matter, including by refraining from attempting to influence any deliberation or action on the transaction or matter, and not be privy to any non-public information relating to the transaction or matter. In the event of such a recusal, the Executive Secretary shall take all necessary action to sequester the employee from the transaction or matter.

The recusal and sequestration of any Board employee from a transaction or matter real or perceived conflict of interest shall be documented by the Office of General Counsel.

I hereby acknowledge that I have read, understand and consent to these policies and procedures:

SIGNATURE **PRINT NAME** **DATE**

NEVADA STATE BOARD OF PHARMACY
OPERATING RESERVE POLICY

1. PURPOSE: It is the fiduciary responsibility of the Nevada State Board of Pharmacy to safeguard the administration of the funds collected and expended in regulating the practice of pharmacy in the State of Nevada. This policy is written to ensure the ongoing financial integrity of the Nevada State Board of Pharmacy.

2. POLICY STATEMENT: Reserves provide a gauge of the financial strength of an agency. Reserves, or undesignated fund balances, are those unrestricted assets which are reasonably liquid and not otherwise budgeted for expenditures. The undesignated fund balance will include an operating reserve to protect the Nevada State Board of Pharmacy when revenues fall short of expenses. To ensure continued and future reliability, this policy proposes to identify a target balance or threshold for the operating reserve.

3. PROCEDURE: The Board will establish an operating reserve out of the undesignated fund balance in an amount not less than six months' operating expenses of the preceding year's budget and not to exceed two years' operating expenses of the preceding year's budget.

4. REVIEW: The operating reserve will be reviewed by the Board on an annual basis and adjusted as necessary. The balance in the operating reservice will be reviewed routinely by the Executive Secretary.

a. When the balance in the operating reserve approaches the six-months' threshold, the Executive Secretary will conduct an evaluation to identify appropriate measures to ensure the continued financial efficacy of the Board. The findings of this evaluation will be submitted at the next regularly scheduled Board meeting. The evaluation will include:

- An examination of the forces affecting funding including a decrease in licensee population, increased services and programs or changes in the regulatory environment.
- A review of expenses to identify if costs can be reduced.
- An evaluation of existing and future potential funding sources.

b. When the balance in the operating reserve approaches the two years' threshold, the Executive Secretary will conduct an evaluation to identify appropriate measures to ensure the threshold is not exceeded. The findings of this evaluation will be submitted at the next regularly scheduled Board meeting. The evaluation will include:

- A review of fee structures.
- An evaluation of expanding services to the extent permitted by law.