FLORIDA DEPARTMENT OF ENVIRONMENTAL PROTECTION

Acknowledgements of Key Policies for Non-DEP Employees

THIS FORM SHOULD BE COMPLETED BY AMERICORPS MEMBERS, INTERNS, VOLUNTEERS OR CONTRACTED INDIVIDUALS ONLY. YOU ARE REQUIRED TO COMPLETE THIS FORM, PRINT, SIGN, AND RETURN THIS STATEMENT TO THE DEP INDIVIDUAL FOR WHICH YOU ARE PROVIDING SERVICES. IT WILL BE RETAINED IN YOUR OFFICE FILE.

Status: Select One

If you selected Americorps Member, complete ALL sections. If you selected any other status, review the Key Directives under SECTION 1, sign and date the bottom of the form before submitting it.

SECTION 1
Acknowledgement of Key Directives

I have reviewed the following key DEP Directives and understand that, if I have questions, it is my responsibility to request clarification from my supervisor or from the Bureau of Human Resource Management:

DEP 202, Code of Ethics
DEP 221, Nondiscrimination Grievance Procedure Directive
DEP 366, Smoking Policy
DEP 390, Information Resources Security Policies and Standards
DEP 375, Records Management
DEP 420, Drug-Free Workplace and Drug Testing
DEP 421, Violence-Free Workplace Policy
DEP 435, Conduct of Employees
DEP 436, Discrimination and Harassment and Sexual Harassment

SECTION 2
Public Records Exemption

Pursuant to Section 119.071(4)(d) specified personal information may be exempted from public record inspection. To claim a personal exemption under the statute, employees must complete the Public Records Exemption Request Form in its entirety and submit a notarized copy to HR_PayrollandBenefits@FlordaDEP.gov before the exemption request will be processed.

Note: All state of Florida employee Social Security numbers, driver's license numbers and medical information (including pre-tax deductions for Division of State group insurance plans) are confidential and exempt from public records inspections.

Public Records Exemption:

- ○ No, I do not meet the criteria for public records exemption.
- ○ Yes, I qualify for public records exemption because I meet one or more of the qualifying criteria for public records exemption.

SECTION 3
Oath of Loyalty

I am a citizen of the state of Florida or authorized non-citizen of the State of Florida and of the United States of America and being employed by or an officer of the Department of Environmental Protection, I am a recipient of public funds and do hereby solemnly declare and affirm that I will support the Constitutions of the United States of America and the State of Florida.

My signature below acknowledges my confirmation to the applicable sections above.

Individual's Signature _____ Date _____

Administrative Directive
DEP 202

Approved by the Secretary
Effective 1-10-2022

Code of Ethics

This directive states policy and establishes procedures for the implementation and administration of a code of ethics within the Department of Environmental Protection (DEP).

AUTHORITY

Ethics, Open Government, and Preventing Sexual Harassment, Executive Order 19-11;
Access to Public Records and Meetings, Article I, Section 24 of the Florida Constitution;
Code of Ethics for Public Officers, Chapter 112, Part III, Florida Statutes;
Public Records, Chapter 119, Florida Statutes;
Disclosure of Financial Interest, Chapter 34-8, Florida Administrative Code;
Executive Branch Lobbyist Registration, Chapter 34-12, Florida Administrative Code; and
Gifts and Honoraria, Chapter 34-13, Florida Administrative Code.

POLICY

DEP is committed to building public trust and confidence, communicating effectively with the public, and maintaining the people's respect. This code of ethics is intended to clearly set forth the Department's ethical principles and expectations in keeping with the Governor's Code of Ethics and support of the code of ethics specified in Chapter 112, Part III, Florida Statutes. To the extent that a statutory provision is not enhanced by a more restrictive, express provision of this Directive, the statutory Code of Ethics shall apply. Therefore, employees should familiarize themselves with the statutory Code of Ethics.

Ethics involves more than simply imposing limits on gifts. This comprehensive DEP Code of Ethics covers a wide range of topics and issues, all of which relate to the ultimate goal of improving services to the public. Promoting the public interest and maintaining the respect of the people in their government is a foremost concern.

ETHICS OFFICER/PUBLIC RECORDS AND OPEN GOVERNMENT CONTACT

The Secretary has designated the General Counsel as DEP's Chief Ethics Officer and public records/open government contact person.

Responsibility of Department's Chief Ethics Officer. The General Counsel is responsible for acting as the Department's contact person for providing information and interpretation concerning ethical issues. The General Counsel will also be the primary liaison between DEP and the Governor's Office of Open Government for purposes of training and compliance. Additionally, the General Counsel has designated an ethics attorney to answer day-to-day questions from DEP employees regarding the DEP ethics code. References in this code to seek assistance from the General Counsel also mean you may contact the ethics attorney.

Responsibility of Public Records and Open Government Contact. The General Counsel is responsible for facilitating access to public records and open meetings. This office is also responsible for providing

information and interpretation concerning any public records issue. Additionally, the General Counsel has designated a public records attorney to respond to legal questions about the public records laws.

Open Government Mediation Program of the Office of the Attorney General. The General Counsel is responsible for acting as the Department's contact person and representative for utilizing this program or similar procedures to expedite resolution of public records and open meeting disputes.

Training. The General Counsel, as the Chief Ethics Officer for the Department, will make reasonable efforts to ensure that training is available regarding ethics, public records, open meeting requirements, records retention, equal opportunity and proper personnel procedures. Please see the People First Talent Management Portal for information on Training Opportunities.

Violations. Employees should report any suspected violations of this DEP Code of Ethics to the Department Chief Ethics Officer (General Counsel), and other appropriate personnel such as a bureau chief, program administrator, director, deputy secretary, DEP Bureau of Human Resource Management or DEP Office of Inspector General.

ETHICS TRAINING

Supervisors are responsible for ensuring that all employees are provided information and appropriate training to ensure full understanding of the Department's Code of Ethics, as specified in this and other related directives. Supervisors shall ensure that they and their employees receive annual training on the subjects of ethics, public records law, open meetings, records retention, equal opportunity, and proper personnel procedures.

Completion of Training. Training for supervisory personnel on the subjects of ethics, public records law, open meetings, records retention, equal opportunity, and proper personnel procedures is available through the Department's Basic Supervisory Training. All supervisors are required to complete this training.

Access to Information. Supervisors are responsible for ensuring that all employees access information on DEP's code of ethics through New Employee Orientation. Editors of DEP's various newsletters are responsible for ensuring that periodic informative articles on DEP's code of ethics provisions appear in these publications. Please contact the General Counsel for assistance.

AVOIDING THE APPEARANCE OF IMPROPRIETY

Use of Power and Resources. Employees must use the powers and resources of the Department to further the public interest and not for any financial or personal benefit other than salaried compensation and employer-provided benefits.

Safeguarding Impartiality. Employees must safeguard their ability to make objective, fair and impartial decisions. Accordingly, employees are prohibited from engaging in any activity or accepting benefits that a reasonable person could perceive as potentially influencing or rewarding their decisions. Employees should

avoid any conduct (whether in the context of business, financial or social relationships) that might undermine the public trust, whether that conduct is unethical or may give the appearance of ethical impropriety. Employees shall consider their circumstances and recuse themselves from certain matters where dealings, finances or personal relationships could lead to the appearance of impropriety. Recusals must be submitted in writing to the Governor's Office of General Counsel after consultation with the Department Chief Ethics Officer (General Counsel). Failure to provide a written recusal when justified may constitute grounds for dismissal.

Conflicts of Interest. Employees whose immediate family relative is a lobbyist are required to report to the General Counsel the names of all such lobbyist's clients quarterly. Such employees are prohibited from participating in any matter that would benefit them or their immediate family relatives, and will refrain from participating in discussions, meetings, or activities involving clients of their immediate family relatives. Directors shall reassign responsibilities that pose a conflict of interest to another employee. Where confidentiality requirements prohibit the public disclosure of any names of clients, the employee must specifically identify the confidentiality concerns prior to or contemporaneously with the submission of the list and the employee's supervising director, in consultation with the General Counsel, will take the measures necessary and appropriate to assure effective recusal by the affected employee(s).

Serving as Officers/Directors of Governmental & Non-Governmental Entities. Contact the General Counsel's designated ethics attorney for further information.

- Employees may serve on the board or commissions of governmental entities subject to the approval of the employee's supervisor and General Counsel.

- No employee may serve as an officer or director of any non-governmental corporation, company, partnership or other entity, regardless of its private or public ownership or its for-profit or item-for-profit status, unless such service meets one of the following exceptions:

  - Subject to the approval of the employee's supervisor and the General Counsel, an employee may serve as an officer or director of a non-governmental, non-profit organization, corporation, company or partnership that does not seek funding by the State.

  - Subject to the approval of the employee's supervisor and the General Counsel, an employee may serve as an officer or director of a non-governmental, non-profit organization, corporation, company or partnership that seeks funding from the State if:

    - ✓ Serving in that capacity is directly related to the employee's employment; and

    - ✓ The employee has been requested to do so by the Secretary of FDEP or is required to serve in that capacity by statute, rule, executive order or other applicable law.

- Subject to the approval of the employee's supervisor and the General Counsel, an employee may serve as an officer or director of a non-governmental, for-profit organization, corporation, company or partnership that does not seek or receive funding from or do business with the State and that is closely-held or family-owned/operated. For example, an employee who, along with other family

members, is an officer or director of an entity that owns rental property could seek approval under this exception.

- Voluntary, pro bono services (i.e., where the DEP employee does not receive compensation) not associated with serving on a board on behalf of non-profit organizations may be permitted, so long as services to such organizations would not have the potential to create a conflict and would not impair the employee's ability to discharge his/her public duties fully and faithfully.

No Personal Benefit. No employee shall participate in an official capacity in any matter that would benefit him or her, or which the employee knows will benefit any family relative or business associate of the employee or family relative.

Screening. To further avoid any appearance of impropriety, employees will not participate in meetings between and/or decisions directly involving the DEP employee and his or her former private employer, clients or business entities for which she or he had substantial, direct responsibility during the two years prior to assuming their present employment with DEP. To the extent the employee seeks to participate in any such meeting or decision, he or she will first notify the supervising Director or equivalent (if the employee is a Director, then his or her direct supervisor) who, with consultation with the General Counsel, will prescribe an appropriate screen depending on the particular circumstances. In no event, however, will a procedure limit the employee's ability to fulfill the core functions of his or her job. Moreover, nothing in this Code is meant to prohibit an employee from addressing or making decisions relating to issues that may generally affect an industry or business sector with which they may have had a prior relationship. For example, a DEP employee may not ever review the permit that he helped prepare as a private engineering consultant, though that DEP employee may review permits that others prepared from the DEP's former employer.

Honoraria and Honorarium Related Expenses. Employees are prohibited from soliciting or accepting, directly or indirectly, honoraria or any other thing of monetary value for speaking appearances or published articles relating to DEP or the employee's DEP employment-related responsibilities. Employees may, however, accept payment of honorarium expenses reasonably incurred. Such acceptance must receive prior approval from the General Counsel. The employee's spouse or relative may not accept any honorarium for expenses incurred to attend such functions with the employee. The employee may not accept payment of honorarium expenses if a political action committee, DEP regulated entity, DEP contractor, a lobbyist, or an employer, principal or partner of a lobbyist offers to pay these honorarium-incurred expenses. However, payment of honorarium expenses reasonably incurred on behalf of the employee by DEP may be reimbursed to DEP and prior approval of these expenses is not required from the General Counsel. See Sections 112.3149 112.3215, Florida Statutes (2019).

Aircraft and Motor Vehicles. The motor vehicles owned, leased, or operated by the Office of the Governor/Lieutenant Governor or any State Department are available for official state business only as authorized by the Governor, Lieutenant Governor, or the Secretary. Although not specifically prohibited by Chapter 112, Florida Statutes, employees are prohibited from traveling in a private aircraft unless they have obtained prior authorization from the Governor or the Governor's Chief of Staff.

Employee Political Activities. Political activities of State employees are restricted by the Federal Hatch Act and Florida law. (See Chapter 110, Florida Statutes). Employees are responsible for being aware of and complying with these restrictions, as specified in DEP 490, Political Activities.

Nepotism. A Specified State Employee is prohibited from seeking for a relative any appointment, employment, promotion or advancement in the unit in which the employee works or over which the employee has control. Employees are responsible for being aware of, and complying with, the provisions in DEP 407, Employment of Relatives. This directive does not prevent relatives from working together in public employment. Contact the Bureau of Human Resource Management for assistance.

Gifts. Nothing of value may be solicited or accepted based upon any understanding that the gift was given to influence official action. (See Section 112.313, Florida Statutes).

The statutory Code of Ethics for public officers, procurement employees and reporting individuals provides that a gift from a lobbyist may not be accepted. (See Section 112.3148, Florida Statutes). However, it is the policy of DEP that no employee, regardless of reporting status, may accept a gift or anything of value from a lobbyist or lobbyist's principal, regardless of whether the item is being offered or given for the purpose of lobbying.

No DEP employee may solicit any gift, regardless of its value, if the gift is for the personal benefit of themselves, their family, or another employee.

Unless given by a relative, any gift received by specified state employees (i.e., reporting individuals and procurement employees, as defined by Section 112.3148, Florida Statutes) which is valued at over $100 must be reported to the Commission on Ethics in the quarter in which it is received. Forms 9 and 10 are available on the Florida Commission on Ethics' website to use for this purpose. (See the section on Financial Disclosure in this directive for more information on financial reporting requirements).

No DEP employee may accept anything of value from a non-lobbyist unless given by a relative or a personal friend in the ordinary course of friendship. A gift from a personal friend may only be given for a special occasion (e.g., holidays, birthdays, weddings, showers, anniversaries, graduation, Valentine's Day, etc.), or as a meal (whether at a restaurant or at a home), or as lodging at the friend's home. However, that personal friend cannot be:

- a lobbyist;
- the partner, firm, member, employer, employee or principal of a lobbyist;
- a person having a special pecuniary interest either individually or through a business entity (e.g., limited liability company, partnership, corporation, etc.) or organization in a matter pending before DEP (e.g., those regulated by DEP) and/or the Office of the Governor/Lieutenant Governor;
- a person who, either individually or through a business entity or organization, provides goods or services to the State under contract or agreement (i.e., a DEP contractor or vendor); or
- a person who, either individually or through a business entity or organization, is seeking to do business with the State.

Gifts, regardless of value, may be accepted on behalf of a governmental entity or charitable organization, or for which a public purpose can be shown, provided the General Counsel has approved such acceptance. DEP employees must contact the General Counsel for assistance with the acceptance of such gifts on behalf of DEP.

Gifts, regardless of value, made to DEP may be accepted by an employee on behalf of DEP provided that the General Counsel has approved such acceptance**.**

In determining whether a gift or potential gift poses a conflict of interest and should not be accepted, the following questions are intended as guidelines for employees.

- Is the gift being given or accepted with the intent that your official action or judgment would be influenced by the gift? If the answer to this question is "yes" the gift, regardless of value, CANNOT be accepted. If the answer is "no" proceed to the next question.

- Do you know, or with the exercise of reasonable care, should you know that the gift is being given to influence your official action? If the answer to this question is "yes" the gift, regardless of value, CANNOT be accepted. If the answer is "no" proceed to the next question.

- Have you accepted multiple gifts, even if nominal in value, from the same source such that the gifts taken in the aggregate may appear that they have been given in circumvention of the prohibition against gifts? If the answer is "yes" the gift CANNOT be accepted. If the answer is "no" proceed to the next question.

- Is the gift being given to you by a relative? If the answer is "yes" the gift CAN be accepted. If the answer is "no" proceed to the next question.

- Is the gift being given by either a registered or unregistered lobbyist, partner, firm, member, employer, employee or principal of a lobbyist, DEP contractor or DEP regulated entity? If the answer is "yes" the gift CANNOT be accepted. If the answer is "no" proceed to the next question.[1]

- Is the gift being given to you by a personal friend, who does not fall into any of the categories specified in this section, in the normal course of friendship for a special occasion or as a meal or lodging? If the answer is "yes" the gift CAN be accepted. If the answer is "no" the gift CANNOT be accepted. Specified state employees must report such gift if it is valued at over $100.00 to the Commission on Ethics (see Quarterly Gift Disclosure under FINANCIAL DISCLOSURE)

- Is the gift being given to your relative by a lobbyist? If the answer is "yes" the gift CANNOT be accepted. Any gift that the DEP employee cannot receive directly may not be received indirectly.

Events sponsored in whole or in part by lobbyist, principal of a lobbyist, DEP contractor or DEP regulated entity.

[1] For a list of registered legislative and executive branch agency lobbyists, see www.leg.state.fl.us/Lobbyist.

- Employees may attend events sponsored by statutory direct-support organizations.

- Employees have a duty to inquire whether an event being offered is sponsored by a lobbyist, principal of a lobbyist, DEP contractor, or DEP regulated entity. Employees may attend events or accept invitations to events sponsored by a lobbyist, principal of a lobbyist, DEP contractor or DEP regulated entity ONLY IF the DEP employee pays or provides equivalent consideration. The payment must be contemporaneous with or precede the receipt of the item or attendance at the event. When such an event is a social occasion, employees should at all times refrain from discussing any State business.

- Employees may attend a community event open to all persons.

- Employees may accept an item or benefit generally available for free or below the customary rate (discount) if the terms or rate is a government rate available to all other similarly-situated government employees or a rate which is available to similarly-situated members of the public by virtue of occupation, affiliation, age, religion, sex, or national origin. This includes free and discounted items or benefits that have been made possible by sponsorship by a lobbyist, principal of a lobbyist, DEP contractor or DEP regulated entity. Prior to accepting any such item, the employee must first determine the discount is available equally to all government employees and is not intended to benefit a particular class of employees. Examples of acceptable free and discounted items or benefits could include:

  - ✓ reduced registration fees for government lawyers attending a legal seminar;

  - ✓ reduced registration fees for government employees attending a chamber of commerce program.

  Such benefits are not "gifts" under this directive or state law.

Awards, plaques, certificates, or similar personalized items given in recognition of the employee's public, civic, charitable or professional service may be accepted if the item has no separate commercial value. If the item is being given by a lobbyist, principal of a lobbyist, DEP contractor or DEP regulated entity the DEP OGC must approve the acceptance.

Exemptions. There may be unique or compelling circumstances warranting exceptions to or waivers from these requirements in certain individual cases. In those instances, prior approval of the General Counsel is required in consultation with the Governor's Office of General Counsel as necessary.

FINANCIAL DISCLOSURE

Specified state employees must comply with reporting requirements.

Disclosure of Financial Interests. Specified state employees are required by Section 112.3145, Florida Statutes, to disclose publicly, by July 1 of each year of state employment, their financial interests to the

Commission on Ethics. See Chapter 34-8, Florida Administrative Code, and Florida Commission on Ethics Form 1 (Statement of Financial Interests). The DEP Bureau of Human Resource Management annually provides a list of specified employees to the Florida Commission on Ethics.

Quarterly Gift Disclosure. Specified state employees must also file a Quarterly Gift Disclosure (Form 9) for all gifts received that are valued at over $100.00. Only those gifts received from relatives or gifts reported pursuant to Form 10 (under Annual Gift Disclosure) are exempted from this quarterly filing requirement.

Annual Gift Disclosure. Specified state employees must also file Form 10, Annual Disclosure of Gifts from Governmental Entities and Direct Support Organizations and Honorarium Event Related Expenses form, to be submitted with Form 1 by July 1 of each year, to report the following:

- any gift valued at over $100 which is received from a governmental entity or direct support organization; or

- actual and reasonable transportation costs, lodging or other expenses related to travel in connection with a presentation made by the employee and paid by a political action committee or lobbyist.

Final Statement of Financial Interests. Specified State Employees must file a Final Statement of Financial Interests (Form 1F) with the Florida Commission on Ethics within 60 days after leaving state employment, unless such employee immediately accepts a subsequent position that requires the employee to comply with the financial disclosure requirements of Section 112.3145, Florida Statutes.

For more information about financial disclosure requirements or to obtain forms, please visit the Florida Commission on Ethics website at www.ethics.state.fl.us. Employees should review regularly their personal assets, business interests and investments to assure that potential conflicts or appearances of impropriety are avoided.

FREQUENT-FLYER MILES AND HOTEL REWARDS POINTS EARNED THROUGH STATE-REIMBURSED TRAVEL

Employees may sometimes be required to travel on State business, requiring them to spend evenings and weekends away from their homes and families. Per diem reimbursements often do not fully reimburse the employee for out-of-pocket travel expenses. As a matter of general policy, any frequent-flyer miles, bonus miles, hotel rewards points, etc. that are awarded to an employee as a result of State-reimbursed travel may be used for personal use by the employee.

DUAL EMPLOYMENT

Secondary employment within state government or outside of state government may not interfere with or pose a conflict of interest with an employee's primary employment with DEP.

Determination by General Counsel. In addition to completing the Notification of Secondary Non-State Employment form and obtaining supervisor approval, Specified State Employees are required to seek an opinion from the General Counsel to determine whether any current or potential secondary employment constitutes a conflict of interest. If the General Counsel determines that the secondary employment constitutes a conflict of interest with the employee's appointment, the employee must sever or not accept the secondary employment relationship. Non-Specified State Employees shall complete the Secondary Employment notification form and obtain their supervisor's approval. (See ADM 401, Dual Employment and Dual Compensation).

Dual State Employment. Non-Specified State Employees may be employed by another state Department in any capacity, in keeping with the provisions specified in ADM 401, Dual Employment and Dual Compensation, and the applicable provisions of collective bargaining agreements. Employees are required to be familiar, and comply, with the provisions of ADM 401.

OTHER PROFESSIONAL CODES OF ETHICS

Nothing in this directive relieves any attorney from any obligations under the Rules of Professional Responsibility; nor shall anything in this directive relieve any professional from any other applicable professional codes of ethics.

DEFINITIONS

Director. Any member of senior management.

Employee. Any DEP employee, regardless of employment classification. [2]

Gift. A service or item having value and accepted, either directly, indirectly, or in trust for the recipient's benefit, by the recipient or by another on the recipient's behalf. Gift includes:

- real property; the use of real property; tangible or intangible personal property or use of such property;
- preferential terms or rate on a debt, loan, goods or services which are not provided as a government rate; forgiveness of a debt;
- transportation; food or beverage; membership dues; entrance or admission fees;
- plants or flowers; personal services for which a fee is normally charged;
- any other similar service or thing having value.

(See Section 112.312 (12), Florida Statutes).

Gift does <u>not</u> include:

[2] DEP has elected to apply the provisions of the lobbying laws contained in Section 112.3148, Florida Statutes, to all DEP employees, rather than limit their application to those individuals who must file financial disclosure forms pursuant to Sections 112.3144 and 112.3145, Florida Statutes.

- salary, benefits, services, fees, commissions, gifts, or expenses associated primarily with the employee's employment;
- except as provided in Section 112.31485, contributions or expenditures, reported pursuant to Chapter 106, contributions or expenditures reported pursuant to federal election law, campaign-related personal services provided without compensation by individuals volunteering their time, or any other contribution or expenditure by a political party or affiliated party committee
- reasonably incurred expenses related to an honorarium event, (see Honoraria and Honorarium Related Expenses of this directive for more on honorarium);
- an award, plaque, certificate, or similar personalized item given in recognition of the employee's public, civic, charitable or professional service,
- an honorary membership in a service or fraternal organization presented merely as a courtesy by such organization;
- use of a public facility or public property, made available by a governmental Department for a public purpose;
- transportation provided to an employee by a Department in relation to officially approved governmental business;
- gifts provided directly or indirectly by a state, regional, or national organization which promotes the exchange of ideas between, or the professional development of, governmental officials or employees, and whose membership is primarily composed of elected or appointed public officials or staff, to members of that organization or officials or staff of a governmental Department that is a member of that organization;
- cash or property received as awards, prizes, or winnings from activities authorized by the laws of this state or other jurisdictions in which such activities, provided that the acceptance of such cash or property does not otherwise pose a conflict of interest as described in this directive, and providing further that the entities or organizations awarding or distributing the awards, prizes, or winnings do not lobby executive branch agencies, do business with DEP (regulated entities or contractors/ vendors), or seek to do business with DEP.

Immediate Family Relative. An employee's spouse, sibling, parent, or child.

Lobbying. Seeking to influence an executive branch Department decision in the area of policy or procurement or attempting to obtain the goodwill of an employee.

Lobbyist. Any person who meets the definitions of that term as used in Chapter 112, Part III, Florida Statutes. Consistent with Section 112.3215, Florida Statutes, "lobbyist" does not include an employee of a Department or of a legislative or judicial branch entity acting in the normal course of his or her duties. Consistent with Chapter 112, Part III, Florida Statutes, a "principal" is anyone (other than a Department, legislative branch entity or judicial branch entity) who employs or retains a lobbyist, either as an employee or independent contractor. The Florida Legislature maintains a website of executive branch lobbyists and their principals and should be consulted by the employee (http://www.leg.state.fl.us). See Sections 112.3215(1)(f)-(i), Florida Statutes (2019).

Relative. An employee's father, mother, son, daughter, brother, sister, uncle, aunt, first cousin, nephew, niece, husband, wife, father-in-law, mother-in-law, son-in-law, daughter-in-law, brother-in-law, sister-in-law,

stepfather, stepmother, stepson, stepdaughter, stepbrother, stepsister, half-brother, half-sister, grandparent, great grandparent, grandchild, great grandchild, step grandparent, step great grandparent, step grandchild, or step great grandchild. Relative also includes a person who is engaged to be married to the subject employee, or who otherwise holds himself or herself out as, or is generally known as, the person whom the employee intends to marry, or with whom the employee intends to form a household, or any other natural person having the same legal residence as the employee. See Section 112.312(21), Florida Statutes (2019).

Reporting Individual (also referred to as a "specified state employee"). An employee who is required to file a financial disclosure form pursuant to Section 112.3144, Florida Statutes. Contact Employee Relations in the DEP Bureau of Human Resource Management to find out whether you are a reporting individual.

Specified State Employee. A reporting individual. See Section 112.3145, Florida Statutes.

This update supersedes DEP 202 dated August 19, 2011 and is necessary to achieve consistency between this directive and the amendments to the Governor's directive as well as clarification to some provisions of this directive.

Please contact the Office of General Counsel for further guidance on any content in this document.

Relevant Forms are available at the Commission on Ethics website.

Administrative Directive
DEP 221

Approved by the Secretary
Effective December 8, 2023

NONDISCRIMINATION GRIEVANCE PROCEDURE

The purpose of this Directive is to establish written guidance for the Department of Environmental Protection (DEP) employees to follow when they receive a complaint alleging discrimination or retaliation by a DEP employee, contractor, program, or activity.

Neither DEP or its employees or contractors may discriminate against any person on the basis of the person's race, color, religion, sex, pregnancy, national origin, age, handicap, or marital status; nor, consistent with DEP 436, Discrimination, Harassment and Sexual Harassment Directive, shall DEP retaliate or intimidate against anyone who exercises their rights or privileges guaranteed by state or federal nondiscrimination laws or opposes an action prohibited under state or federal nondiscrimination laws. This prohibition includes programs for which DEP is receiving or administering appropriated funds.

By virtue of receiving funding, DEP, including its employees and contractors must comply with the following civil rights laws and regulations:

- Title VI of the Civil Rights Act of 1964 as amended (prohibiting discrimination in federally assisted programs on the basis of race, color, or national origin in the delivery of services or benefits);
- Section 13 of the 1972 Amendments to the Federal Water Pollution Control Act (prohibiting discrimination on the basis of sex in the delivery of services or benefits under the Federal Water Pollution Control Act as amended);
- Section 504 of the Rehabilitation Act of 1973 (prohibiting discrimination in federally assisted programs on the basis of disability, both in employment and in the delivery of services and benefits);
- Age Discrimination Act of 1975 (prohibiting discrimination in federally assisted programs on the basis of age in the delivery of services or benefits);
- 40 C.F.R. Part 7 (implementing Title VI of the Civil Rights Act of 1964, Section 13 of the 1972 Amendments to the Federal Water Pollution Control Act, and Section 504 of the Rehabilitation Act of 1973); and
- Part I, Chapter 760, F.S. (prohibiting discrimination on the basis of race, color, religion, sex, pregnancy, national origin, age, handicap, or marital status).

FILING A COMPLAINT

1. A person who thinks they have been discriminated against by an employee or contractor of DEP on the basis of race, color, religion, sex, pregnancy, national origin, age, handicap, or marital status, or thinks they have been retaliated against for having engaged in protected activity, may file a complaint with the DEP's Inspector General using the Complaint of Discrimination form. This form is available in English, Spanish and Haitian Creole. Complaints may also be made by using the contact information for the Inspector General listed below.

Contact Information for the DEP's Inspector General is:

Candie M. Fuller, Inspector General
Office of Inspector General
3800 Commonwealth Blvd.
MS #40
Tallahassee, FL 32399
Email: Candie.Fuller@floridadep.gov
Phone: (850) 245-3151

2. Pursuant to Section 20.055, Florida Statutes, the Inspector General serves as DEP's "central point for coordination of and responsibility for activities that promote accountability, integrity, and efficiency in government." The DEP Inspector General Office is charged with, among other things:

- Providing direction for, supervising, and coordinating audits, investigations, and management reviews relating to DEP programs and operations for the purpose of detecting, deterring, preventing, and eradicating misconduct and other abuses within DEP; and
- Reviewing rules and policies relating to DEP programs and operations and making recommendations concerning their impact.

See Section 20.055(2) & (7), F.S.

3. In carrying out these duties, the DEP Inspector General must comply with the General Principles and Standards for Offices of Inspector General as published and revised by the Association of Inspectors General; and the DEP Inspector General is protected from any actual or perceived impairment to their independence including the freedom from any interference with investigations and timely access to records and other sources of information. *See* Section 20.055(2)(j) & (7)(d), Fla. Stat.

5. The General Principles and Standards for Offices of Inspector General ensure, among other things, that the DEP Inspector General provides his or her staff with direction, guidance, oversight, and training and follows the basic principles of integrity, objectivity, independence, confidentiality, professionalism, competence, courage, trust, honesty, fairness, forthrightness, public accountability and respect for others and themselves when conducting investigations, reporting, and carrying out their additional duties.

RESPONSE

1. An employee, or contractor of DEP who receives a complaint that an employee, or contractor, of DEP has allegedly participated in discriminatory or retaliatory conduct shall notify the Inspector General as soon as practical.

2. Upon receipt of a complaint, the Inspector General shall adhere to the investigatory process and responsibilities enumerated in DEP 290, Internal Investigations Directive, which includes a process for timely, thorough and fair investigations, that are free from impairment, and related procedures for documentation, tracking, and reporting.

EXTERNAL COGNIZENT AGENCY

DEP encourages individuals to file complaints of the kind discussed in this directive with the Inspector General. However, this directive is not intended to prevent individuals from seeking remedy under state or federal law.

If an individual feels he or she has been discriminated against on the basis of race, color, religion, sex, pregnancy, national origin, age, handicap, or marital status, or alleges retaliation for having engaged in protected activity, a complaint may be submitted to:

U.S. Environmental Protection Agency
Office of External Civil Rights
Mail Code 2310A
1200 Pennsylvania Ave, NW
Washington, D.C. 20460
Email: Title_VI_Complaints@epa.gov

AGREEMENTS

DEP will not enter into agreements nor continue existing agreements with any organization that knowingly discriminates against any person on the basis of race, color, religion, sex, pregnancy, national origin, age, handicap, or marital status or that retaliates or intimidates against anyone who exercises their rights or privileges guaranteed by state or federal nondiscrimination laws or opposes an action prohibited under state or federal nondiscrimination laws.

DISTRIBUTION

A copy of this directive will be made available to all DEP employees or contractors. A copy will also be provided in orientation materials provided to new employees of DEP. This directive will also be posted on DEP's website, https://floridadep.gov/sec/sec/content/equal-opportunity-nondiscrimination. The directive will be reviewed by the DEP Inspector General's Office on a continuous basis and updated as necessary.

FLORIDA DEPARTMENT OF ENVIRONMENTAL PROTECTION		
ADMINISTRATIVE POLICY		
	TITLE: **Smoking Policy**	POLICY: **ADM 366** EFFECTIVE DATE: **8-4-2022** Established:
REFERENCES: Smoking and Vaping, Chapter 386, Part II, Florida Statutes (F.S.)		

PURPOSE/SCOPE

Establishes Department policy regarding smoking to protect all individuals in the Department of Environmental Protection (DEP) owned, leased and managed facilities from the health hazards of secondhand tobacco smoke, and in compliance with the Florida Clean Air Act.

POLICY

Smoking (including e-cigarettes, vapor-inhaling products, etc.), is prohibited at all times in all buildings and main entryways, which are owned or leased by the Department of Environmental Protection. Smoking is prohibited at all times in all DEP vehicles. At the request of smokers, breaks shall be granted during trips but the number and duration shall not exceed employee break periods allowed by Directive DEP 425, Attendance and Leave. Violations of this directive or the Florida Clean Air Act may result in disciplinary action pursuant to DEP 435, Conduct of Employees. All persons offered employment shall be advised of this policy prior to employment. The Bureau of Human Resource Management (HR) shall provide access to this directive in each new employee information packet.

DESIGNATED SMOKING AREAS

Individuals may only smoke in designated smoking areas. Designated smoking areas for all DEP owned, leased and managed facilities will be positioned no less than 30 feet from the primary entrance door(s) of the facilities. Individuals are prohibited from smoking in non-designated areas, including the front, back and side entryways of facilities. Ashtrays located outside facility entrances are exclusively for use by visitors to dispose of tobacco products before entering the facility. The presence of ashtrays alone does not designate a smoking area or otherwise serve to permit smoking in the vicinity.

POLICY MAINTENANCE ADMINISTRATOR

This policy is maintained by the Director of Administrative Services

STANDARDS

There are no separate administrative procedures or forms associated with this policy.

Administrative Directive
DEP 390

Approved by the Secretary
Effective: 8-23-2024

INFORMATION TECHNOLOGY RESOURCE SECURITY

The purpose of the Information Technology Resource Security Directive is to ensure that the security of DEP's information resources is sufficient to reduce the risk of loss, modification, or disclosure of department IT assets. The department's adherence to these policies ensures compliance with the State's information security rules and offers DEP a set of best practices that assures the security of information under the department's responsibility to protect. Information security policies and standards apply to all DEP employees, contractors, vendors, private organizations, and citizens that are provided account access to the DEP network and computer systems regardless of how or where they connect.

AUTHORITY

Security of Data and Information Technology Section, Chapter 282.318(3) and (4), Florida Statutes
Information Technology Standards, Chapter 60 GG-2, Florida Administrative Code

RESPONSIBILITIES

All Computer Users/Workers (Employees, Contractors, Volunteers, other users)

- This directive includes multiple focus areas which pertain to different programs, organizations, and areas of responsibility. However, the following sections and statements pertain to all computer users* and must be acknowledged in the DEP Computer User Statement of Understanding as stated in section IA of this policy:
  - I-A: Prior to Employment
  - I-B: During Employment
  - I-D: Acceptable Use of IT Resources and the Internet
  - II-A: Use of Technology Assets
  - IV-B: User Access Management and Responsibility
  - IV-E: Password Usage
  - IV-G: Mobile Computing and Remote Access Control
  - V-B: Computer Network Usage
  - V-E: Network Monitoring
  - VIII-A: Reporting of Information Security Incidents
  - IX-B: Backup and Recovery
  - X-A: Compliance
  - X-B: Exceptions to the Security Policies

  *IT Workers (OTIS staff, IT contractors and District Analysts) must read and acknowledge the entire directive.

Information Security Manager (ISM)

- Development of a strategic information security plan and associated operational information security plan.
- Development, implementation, and update of agency security policy, procedure, standards, and guidelines.
- Development and implementation of the agency security awareness program.
- Coordination of the agency information security risk management process.

- Coordination of or assisting the Inspector General in the coordination of the agency Computer Security Incident Response Team.
- Coordination of Information Technology Disaster Recovery efforts in support of the agency Continuity of Operations Plan.
- Taking an active role in the agency information technology (IT) monitoring and reporting activities.
- Maintaining information security program documentation and policies

Owner, Custodian and User Identification

- Owners, custodians, and users of all information resources will be identified, and the designation will be documented.
- All information resources will be assigned a data owner.
- The owner of an information resource is the designated individual responsible for managing the uses of the resource. The owner is responsible for:
  - Approving access and formally assigning custody of the resource.
  - Judging the resource's value.
  - Specifying data control requirements and conveying them to users and custodians.
  - Ensuring compliance with applicable controls.
  - Defining rules to ensure the quality of the data.
- The custodian of an information resource is responsible for:
  - Implementing the controls specified by the owner to ensure integrity of data.
  - Ensuring the availability of data.
  - Providing physical and procedural safeguards for the information resources in their possession or in their facility.
  - Administering access to the information resources.
  - Serving as security authority and system administrator for all information resources.
  - Providing for timely detection, reporting, and analysis of unauthorized attempts to gain access to information resources.
  - Assisting owners in evaluating the cost-effectiveness of controls.
- The users of information resources are responsible for:
  - Complying with controls established by the custodian.
  - Preventing disclosure of confidential information.

External Parties and Contracts (Contractors, Vendors, and Partners)

- Contracts and agreements involving the use of agency's IT resources will require compliance with the agency IT security policies and procedures.
- Before any third-party network, software or device is permitted to connect to the agency network, a review and approval must be provided by the department's ISM.
- The agency ISM is responsible for maintaining network connection agreements.
- The agency shall maintain procedures to ensure that security requirements are specified throughout the procurement process for IT services.

I. HUMAN RESOURCE REQUIREMENTS

OBJECTIVE

The Human Resource requirements establish protective measures for the use of DEP IT resources by ensuring employees, contractors, vendors, volunteers, and business partners understand their roles and responsibilities, and that they are suitable for the positions for which they are being considered. Users of all DEP IT resources will be provided with training on information security threats and concerns and their responsibilities and liabilities. Also, upon termination of employment, all DEP IT resources shall be returned, and all access rights removed.

CONTROL

The Bureau of Human Resource Management (BHRM) is responsible for providing accurate job descriptions and addressing security responsibilities as it relates to terms and conditions of employment. All candidates for employment will be adequately screened, especially for positions of special trust. Furthermore, management will require employees, contractors, and other users, to apply security in accordance with established policies and procedures of the agency.

SCOPE AND POLICY

This Human Resource Security Policy applies to all employees, contractors and anyone using agency IT resources.

A. Prior to Employment (Applies to all Computer Users/Workers)

1) Upon employment, employees, contracted staff, and volunteers shall acknowledge their responsibility to review, request further clarification from their supervisor or from the BHRM and comply with this directive upon electronic acknowledgment of the DEP Key Directives. The BHRM will maintain this acknowledgment in the employee's official personnel file. The division obtaining the contracted services will keep the acknowledgment of DEP Key Directives with the work contract and maintain a record of these documents.
2) All IT positions, including contractors providing IT services, will be classified as positions of special trust requiring background checks and level 2 screening in accordance with DEP 422, Positions of Special Trust, or Responsibility. Positions of special trust are set forth in Section 110.1127, and Chapter 435, Florida Statutes.
3) For contractual employees, the Division initiating the contract is responsible for ensuring that a level 2 background check is complete and cleared before work can begin.

B. During Employment (Applies to all Computer Users/Workers)

1) The BHRM will designate positions of special trust based upon job duties. Employees in these positions will receive additional training related to their level of security access.

2) Contractors, vendors, and partners contracted with the agency or acting on behalf of the agency shall comply with agency security policies and employ adequate security measures to protect agency information, applications, data, resources, and/or services.

C. **Security Awareness and Training**

1) Workers shall receive initial security awareness training within 30 days of employment start date.
2) Records of individuals who have completed security awareness training will be maintained.
3) Agency requires all employees and contractors to participate in annual cybersecurity training to include on-going education and reinforcement of security practices.
4) Special trust positions will be adequately trained to carry out their assigned information security-related duties and responsibilities.
5) Initial training shall include acceptable use restrictions, procedures for handling confidential and exempt information and computer security incident reporting procedures.
6) Security training specific to an application is the responsibility of the application owner.
7) Designated individuals will be trained to maintain computer environmental controls systems and properly respond in case these systems fail.
8) The ISM will ensure an ongoing information resource security awareness program is available to keep all users accessing computer systems up to date regarding new or changing security policies and responsibilities relating to their use of State information resources.

D. **Acceptable Use of IT Resources and the Internet (Applies to all Computer Users/Workers)**

1) DEP shall have sole discretion to determine whether the use of an IT resource use is personal, or business related.
2) Personal use shall not interfere with the normal performance of a worker's duties.
3) Activities such as banking, shopping and conducting other personal financial transactions using DEP resources are not permitted.
4) Workers will access only IT resources and information to which they have authorization or explicit consent.
5) Workers will refer to DEP Ethics Directive 202 regarding the use of IT resources for profit or political activities.
6) Detailed information about security configuration will only be released to authorized individuals and/or groups.
7) Computer users shall have no expectation of privacy with respect to the contents of agency-owned or agency-managed IT resources.
8) All users are expected to conduct themselves with the highest integrity when using Internet resources. Use of the Internet is subject to monitoring by IT security and upper management. Use of the Internet is permitted as long as:
   - Personal use of the Internet is limited to scheduled breaks and lunch hour.
   - Employees are responsible for exercising good judgment regarding the web sites they visit.
   - Personal use does not interfere with normal business activities.
   - The user performs no activity that violates federal, state, or local laws or would otherwise be prohibited under rules in the Florida Administrative Code (F.A.C.).

- The user does not deliberately use peer-to-peer file sharing, websites/software associated with hacking, cracking, or other illegal cyber activities. Users will not access inappropriate Internet resources such as those containing material relating to gambling, illegal drugs, illegal drug paraphernalia, hate-speech, violence, pornography, and sites containing obscene materials.

E. **Termination of Employment**

1) Access authorization shall be removed when the user's employment is terminated or access to the information resource is no longer required.
2) Upon the voluntary or involuntary termination of an employee, or upon notification to the employee of impending termination, any application owners will ensure all access authorizations are revoked and will take custody of, or ensure the safe return, modification, or destruction of all of the following items assigned:
   - Collect keys and identification badges.
   - Change system passwords and lock combinations.
   - Collect confidential data and documentation, along with operator procedures, and other sensitive program documentation and manuals.
   - Collect or account for state-owned computers, software, and any state issued assets/property.

II. IT ASSET MANAGEMENT SECURITY

OBJECTIVE

To ensure accountability and maintain appropriate protection of the organization's assets, all DEP IT assets will be accounted for and have a designated owner. The implementation of specific controls for IT assets may be delegated by the owner as needed, but the owner remains responsible for the proper protection of the assets.

CONTROL

All agency IT assets will be identified, classified, and inventoried for accountability and control of assets to allow for proper data protection and asset maintenance.

SCOPE AND POLICY

The scope of the IT Asset Management Security Policy applies to all employees and anyone responsible for agency IT resources, and this policy includes the sections of Technology Asset Use, IT Asset Management, and Information Classification and Confidentiality.

A. Use of Technology Assets (Applies to all Computer Users/Workers)

1) All hardware owned or managed is considered the property of the agency. The agency may inspect any files stored on agency internal network or computer systems, including attached removable media.
2) All data and information generated by employees for agency use is considered agency intellectual property legally owned by the agency.
3) Only software owned/licensed by the agency and approved freeware may be installed on agency computers. All software installation requests must be submitted through the OTIS Service Desk for installation by an OTIS technician or a division/district designee approved by the Service Desk. Justification and supervisory approval must be included in all software installation requests. All other employees may not install software on agency computers. Trial, demo, or evaluation software must be removed or purchased at the end of the trial period.
4) Copies of state-owned, leased, or licensed software should not be created, kept, or installed on any DEP computer system if such copying violates the copyright or the license agreement with the software vendor.
5) Non-agency managed and personally owned hardware or software is prohibited from being connected to or installed on agency computers unless approved by the CIO after consultation with the ISM. At no time shall confidential information be allowed to be transported or stored on a personally owned asset.
6) Unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of IT resources is prohibited.
7) Workers in control of sensitive assets and information must secure resources while not in use.
8) Computer users will not disable, alter, or circumvent agency workstation security measures.
9) Computer users shall take precautions to protect mobile computing devices in their possession from loss, theft, tampering, unauthorized access, and damage.
10) Employees will report loss of any IT assets immediately to the Service Desk.

11) Employees will immediately report lost security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes.
12) Hardware and peripheral devices must be kept safe from physical harm including accidental damage, theft, abuse, or loss.
13) Employees must obtain authorization from their supervisor with documentation of equipment required to function to the DEP property custodian before taking IT equipment, software, or information away from the agency facility.

B. **Information Technology Asset Management**

1) To ensure IT resources are properly maintained and accounted for, hardware and software inventories must be maintained by each division, district, and office to allow ready access to the data by the respective technicians and managers.
2) Software, licenses, proofs of purchase, and media shall be controlled by the designated software asset custodian within the respective division. For software programs requiring the media to reside at the user's workstation, the user is accountable for ensuring the media is not illegally copied and is readily available if needed by the Service Desk.
3) All electronic devices and media must be re-imaged or formatted (using full format process) as appropriate prior to being reassigned within DEP. Removable or external drives used solely for the transfer of data between computers are exempt unless being repurposed or disposed of.
4) In the case of asset disposal, DEP 55-406, Certification of Surplus Property form, must be completed to document the name of the person sanitizing and sanitization method. Forms of acceptable methods of sanitization include using agency-approved software to overwrite data on computer media, degaussing, or physically destroying media. ADM 320, Property Policy provides procedures for surplus disposal.
5) Procedures for sanitization of agency-owned computer equipment, corporate mobile devices and any other electronic device that contains a hard drive must be adhered to. Refer to the Sanitization Procedures on DEPnet for further information.

C. **Information Classification and Confidentiality**

1) Information classification will categorize IT resources according to the Federal Information Processing Standards (FIPS) Publication 199. This process estimates the magnitude of harm that would result from unauthorized access, unauthorized modification or destruction, or loss of availability of a resource: low-impact, moderate-impact, or high-impact relative to the security objectives of confidentiality, integrity, and availability.
2) Information and software that is deemed confidential or exempt from disclosure will be identified under provisions of applicable state and federal laws.
3) Confidential and exempt information will be protected using appropriate administrative, technical, and physical controls (e.g., passwords, user IDs, firewalls, encryption).
4) Data owners are responsible for identifying and classifying information. Data owners will work with their division or office's Data & Analytics Governance data steward to log key data assets in the DEP data catalog. The data steward will include the classification and all required metadata in the DEP data catalog.
5) Procedures for handling and protecting confidential and exempt information will be referenced in the Information Security Plan where applicable.

6) Agreements and procedures must be in place before sharing, handling, or storing confidential data with entities outside DEP.

III. PHYSICAL AND ENVIRONMENTAL SECURITY

OBJECTIVE

Employees' access to DEP facilities, data, and phone wiring, electrical, heat, air conditioning and ventilation controls must be managed in a way to prevent loss, damage, or compromise to IT resources. This policy section establishes the rules and procedures that are implemented to secure physical and environmental factors around IT resources.

CONTROL

This policy exists to prevent unauthorized access, damage, compromise and interference to agency premises and information, assets, agency activities, and facilities.

SCOPE AND POLICY

The Physical and Environmental Security Policy applies to all employees and anyone accessing agency IT resources, facilities, administrative equipment, and infrastructure.

A. Secure Areas (Work, Production and Lab, and Off-Premises)

1) All personnel admitted into restricted agency work areas must have an access control key badge (card) or be signed in by a person authorized to admit visitors. Personnel may not bypass sign-in procedures to admit anyone to DEP facilities. Control of physical access to the workplace provides protection for IT resources.
2) Physical controls shall be appropriate for the size and criticality of the IT resources.
3) Access to telephone wiring closets, IT resources machine rooms, network switching rooms, as well as areas containing sensitive and confidential information must be physically restricted.
4) Access to the computer data centers, server rooms, and closets housing network infrastructure equipment will be restricted to those responsible for maintaining these operations or related equipment. Visitors shall be recorded and supervised where appropriate. The System Administrator is responsible for determining which vendor maintenance/service personnel may be allowed to work without staff escort.
5) Management responsible for the staff working in restricted areas must ensure an appropriate access control method (receptionist, metal key and combo locks, magnetic card readers and door locks) is employed.
6) The security policies outlined in this document are also applicable at remote locations and facilities, even though the appropriate method implemented to control these areas may vary based on location or facility.

B. Equipment Security

1) IT infrastructure must be placed in locked cabinets, locked closets, or locked computer rooms.
2) Electrical, data, and voice network wiring must be planned and installed under the supervision of authorized individuals. Other personnel may not alter, move or remove existing wiring.

3) The temperature and humidity within a central computer room will be monitored and controlled to ensure that the operational environment conforms to the manufacturer's specifications.
4) Heating, ventilation, and air conditioning (HVAC) facilities must be maintained by authorized personnel. Non-authorized personnel may not modify controls, settings, or implement HVAC equipment.

IV. ACCESS CONTROL

OBJECTIVE

Only authorized individuals will gain access to agency information resources to perform official business, while minimizing the risk and subsequent impacts of unauthorized access or effect of such. This will be achieved by restricted access privileges of all users, systems, and automated processes based upon the 'least privilege' concept, in which a legitimate business requirement for access is granted and authorized by the appropriate management personnel.

CONTROL

These policies describe the requirements for access to information and prevent unauthorized access to information systems to ensure protection of networked services; to prevent unauthorized computer access and activities; and to ensure information security when using remote access.

SCOPE AND POLICY

The Access Control Policy applies to all employees and anyone accessing agency IT resources. This policy is broken up into the following sections: Business Requirements for Access Control; User Access and Management Responsibility; Network Access Control; Password Administration and Use; Service Accounts, and Mobile Computing and Remote Access Control.

A. Business Requirements for Access Control

1) Administrative rights for IT resources should be restricted to IT workers who have received appropriate technical training and who are authorized based on job duties and responsibilities.
2) Identify users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to agency information and IT resources.
3) Administrative account activities shall be traceable to an individual. Each user of an information resource accessible by multiple users will be assigned a unique user identification and password.
4) Workstations and mobile computing devices shall have a screensaver enabled and secured with a complex password and with the automatic activation feature set at no more than 15 minutes. The CIO and Information Security Manager may allow exceptions as needed for operations.
5) Non-DEP individuals must first be authorized by an appropriate DEP representative, within established procedures, before access is given.
6) Before a non-DEP individual is granted access to an IT resource, the appropriate Systems or Application Administrator will review the request and grant access and will notify Information Security when the access request seems inappropriate.
7) Upon the decision to terminate an employee or an employee resignation, the Bureau of Human Resource Management and/or responsible program area will follow established processes and procedures to make sure that the employee's access to facilities and IT resources is revoked in a timely manner.

8) Access accounts assigned to an individual will not be used in automated production programs, queries, scripts, or other automated system or operational processes. Instead request a service account for automated access to IT resources.
9) Modifying, changing, or updating access privileges to DEP IT resources via shared passwords or group accounts is prohibited.
10) Only authorized individuals will have authority to change permission levels on servers, network devices, server directories or folders, databases, or other IT resources.
11) Access privileges for network user accounts assigned to an individual that have been found to be inactive for more than 60 days will be locked/disabled and can only be unlocked/re-enabled by authorized IT personnel.
12) Access privileges will be set according to a "least privilege" principle in which the level of access provided syncs up with the job functionality.
13) Security requirements for network connection resources must include consideration for the interaction resources have with other systems on the network and Internet.
14) Application Owners will review access rights every six months based on risk, access account change activity, and failed login rate.
15) Accounts with administrative rights must be created, maintained, monitored, and removed in a manner that protects IT resources.
16) Elevated access accounts must be independent from a user's primary network account.
17) Application Owners are responsible for authorizing access to information.

B. **User Access Management and Responsibility (Applies to all Computer Users/Workers)**

1) Employees may not hack, capture, or otherwise obtain passwords, encryption keys or any other access control mechanism without approval from the Information Security Manager. Employees found to have violated this directive will be subject to immediate disciplinary action, up to and including termination of employment.
2) Employees will not attempt to access data or programs housed on IT resources that are not part of their job function, and where authorization or explicit consent has not been granted.
3) Users will be held accountable and responsible for activities that occur under their assigned user ID.
4) Employees shall not share their agency accounts, passwords, personal identification numbers, security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes with anyone.
5) Based on their role, workers shall be authorized access to IT resources based on the principle of "least privilege".
6) Personnel must logout or lock out access to their workstations for all IT resources when leaving their work area.

C. **Network Access Control (Login/Logout)**

1) A computer user with access to the network will have a unique user account ID and password.
2) System Administrators must ensure accounts with administrative rights are created, maintained, monitored, and removed in a manner that protects IT resources.
3) All network access (including wireless) shall require user authentication.

4) Scripts implementing automated access that attempts to bypass subsequent authentication or apply blanket authentication to multiple machines that are attached to the network are not permitted without approval by the Information Security Manager.
5) Where systems have the capability, IT resources will record all login attempts.

D. **Password Administration**

1) All IT resources connected to the network, either permanently or intermittently, must have password access controls. The agency shall not use vendor-supplied default passwords.
2) Passwords must be changed immediately after a security breach has been detected to the affected systems.
3) If there is any reason to believe that a password has been disclosed to anyone other than the authorized user or compromised in any way, the account will be disabled.
4) Default, initial, or reset passwords will not use or contain simple passwords like 'newuser1', or 'password1' in any form or order, must comply with established password policy, and must be changed after first login.
5) As the system software permits, an initial or reset password issued to a user will be valid only for the user's next login, after which the user must be prompted to change their password.

E. **Password Usage (Applies to all Computer Users/Workers)**

1) Passwords assigned to individuals must not be shared or revealed to anyone including a supervisor, upper management, or technical support personnel. The users to whom passwords are assigned shall protect the passwords from disclosure and must refuse the identification of all other users' passwords.
2) Passwords will not be stored in readable form (clear text) in batch files, automatic login scripts, software macros, or terminal function keys, and except for one-time passwords should not be transmitted via email.
3) Privileged user IDs and passwords are not to be hard coded or saved in scripts, login procedures or databases unless approved by ISM and stored in a secured location. An individual must authenticate before executing manual scripts.
4) Passwords must be strong and complex in design and will have these minimum characteristics:
   - A length of at least twelve characters.
   - Contain three of the following four: uppercase letters, lowercase letters, numbers, symbols.
   - Cannot be same password as any of the last 5 passwords used.
5) Passwords for IT resources will be set to expire every 180 days or must be reset at least every 180 days.
6) User network accounts will be locked after five unsuccessful attempts to enter a password, within 15-minutes.

F. **Service Accounts**

1) Service accounts must be maintained in a manner that protects IT resources.
2) Service accounts may be exempted from agency password expiration requirements.
3) Service accounts shall not be used for interactive sessions.
4) Unique service accounts will be established for all production systems that require access to IT resources that are account and password protected.

5) For automated access to IT resources, System Administrators must request and use service accounts.

G. **Mobile Computing and Remote Access Control (Applies to all Computer Users/Workers)**

1) DEP owned mobile computing devices must be tracked and users assigned these resources must sign a responsibility statement as established by the ISM.
2) Employees must take precautions to protect mobile computing devices in their possession from loss, theft, tampering, unauthorized access, and damage.
3) Mobile computing devices shall require user authentication before access is allowed on the device when used in a mobile, non-DEP network environment.
4) Mobile computing devices containing confidential information shall be encrypted using agency-approved encryption software or methods.
5) Windows devices must be firewall protected when connected to a non-agency network.
6) Users may remotely connect computing devices to the agency network only through agency-approved, secured remote access methods.
7) Remote access client connections shall not be shared.
8) Only authorized IT personnel may provide Virtual Private Network addresses.
9) All remote connections will require user authentication before gaining network access.
10) Confidential information transmitted over the Internet must be encrypted.

V. NETWORK AND OPERATIONS MANAGEMENT

OBJECTIVE

The Network and Operation Management Policy is designed to protect the operating environment and network in 'real-time'. These policies are developed to also promote a stable and consistent service for all IT resources. The purpose of this policy is to maintain the integrity and availability of information; ensure the protection of information in networks, including those networks that may span agency boundaries; maintain the security of information and software exchange within the agency; and make sure that systems are audited and monitored for unauthorized information processing activities.

This policy for securing IT resources is intended to be a reference to which Administrators must adhere but is not intended to circumvent Administrators' use of sound judgment and creativity in matters of security.

CONTROL

DEP will monitor, control, and protect agency information when transmitted across the agency's network infrastructure.

SCOPE AND POLICY

The Network and Operations Management policy applies to all personnel and anyone using agency IT resources. This policy is broken up into the following sections: Operational Management and Responsibilities; Computer Network Usage, Network Security Management; and Audit and Monitoring.

A. Operational Management and Responsibilities

1) Virus checking software must be approved by OTIS and will be deployed on all systems susceptible to virus, and on all servers. These programs must be continuously enabled, updated and configured so non-Administrators cannot disable them. Externally supplied software media may not be used on any computer running a Windows or Linux/Unix operating system unless it has been virus scanned. Furthermore, personnel may not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce computer code designed to self-replicate, damage, or otherwise hinder the performance of or access to any IT resource.
2) Computer operating system and application hot fixes, service releases, and patches shall be installed on applicable computer systems in a timely manner in accordance with agency patch management guidelines. The status of these maintenance updates shall be maintained to facilitate the task of ensuring required updates are completed for all applicable systems within the designated timeframe. The National Institute of Standards and Technology (NIST) procedures for Handling Security Patches, Special Publication 800-40, can be used as a guide.
3) The login prompt for IT resources must not reveal specific information about the agency, the network configuration, or other internal information until the user has successfully logged in.
4) In the case of login failure, the user must not be given any specific feedback indicating the source or type of failure, but instead just be informed that the process has failed.

5) Non-Administrators must contact the Service Desk to request the installation or upgrade of any application software on DEP workstations.
6) The application development, test, and production infrastructure should be physically or logically separated.
7) IT resources shall be validated as conforming to agency standard configurations prior to production implementation.
8) Production confidential data shall not be used for testing or development. Copies of production data will not be used for testing unless the data has been desensitized or unless all personnel involved in testing are otherwise authorized access to the data.
9) All application changes will go through change control management procedures and be approved before implementation to determine whether they have been authorized, tested, and documented.
10) Development and test environments will not be permitted to establish connection with any production resource except under change control procedures. Any ongoing access between these environments and production must be documented and presented to the ISM for approval for continued use.
11) Desktop Support will design minimum configuration images for desktops and laptops so that all implementations of the operating system and application suite for a particular job function are identical.
12) System Administrators will devise a standard build process and minimum-security configuration, and ensure implementation is identical for servers sharing the same process and functionality.
13) OTIS will develop and maintain a list of approved applications for agency computers.
14) Job functions susceptible to fraudulent or other unauthorized activities must have 'separation of duties' so that no individual has the ability to control the entire process of those functions.

B. **Computer Network Usage (Applies to all Computer Users/Workers)**

1) No personally owned devices (e.g., MP3 players, USB storage device of any size, printers) shall be connected to state-owned IT resources unless approved by the Service Desk.
2) Users must not extend or re-transmit network services in any way. This means no router, switch, hub, or wireless access point may be connected to the agency network without OTIS approval.
3) Only agency-owned or agency-managed IT resources may connect to the agency network; and only agency-owned or agency-managed mobile storage devices are authorized to store agency data without approval from the ISM.
4) Only OTIS System Administrators can change folder admin access privileges for networked file storage.
5) Only agency approved wireless devices, services, and technologies may be connected to the agency network.
6) DEP Virtual Private Networks (VPNs) may only be accessed by DEP-owned resources or where an exception has been authorized by the ISM or CIO.
7) It is inappropriate to use email or other messaging functions for the distribution of malware, forging headers, propagation of "chain" letters, and auto-forwarding agency messages to a non-agency address.
8) Employees shall use only approved electronic mail services when using DEP resources.
9) Approved email services may not be used for unlawful activities, commercial purposes not under the auspices of the agency, personal financial gain or uses that violate other agency policies or guidelines.
10) Employees shall not use email services to represent, express opinions, or otherwise make statements on behalf of DEP or any unit of the agency unless authorized to do so.

11) Employees shall not use email services for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing resources, or unwarranted or unsolicited interference with the use of email or email systems by others (e.g., animated email signatures).
12) Both the law and DEP policy prohibit the theft or abuse of computing resources. These prohibitions apply to email services and include unauthorized entry, use, transfer, or tampering with the accounts and files of others, interference with the work of others and with other computing resources or facilities.
13) Employees shall not use email services to access, send, store, create or display inappropriate or illegal content, including sexually suggestive or explicit material, gambling, profanity, political activities, obscenity, harassment or discrimination regarding age, race, color, sex, religious belief, national origin, political opinion, or disability.
14) DEP email addresses are only to be used for DEP business purposes.
15) Employees shall not send mass emails unless authorized. This restriction does not preclude an employee from sending multiple emails to a group for official business. Large attachments with graphics, video files, or sound effects are discouraged.
16) If an employee believes an unsolicited email may be attempting to compromise agency systems or data, it should be reported by using the Phish Report Button in Outlook.
17) Email is subject to the full range of laws applying to other communications, including copyright, breach of confidence, defamation, privacy, contempt of court, harassment, anti-discrimination legislation, the creation of contractual obligations, and criminal laws.
18) Personally Identifiable Information (PII) shall not be transmitted via email for personal purposes.

C. **Network Security Management**

1) Firewall and router configuration standards must be established and include a current and complete network diagram with IP addresses and subnet masks.
2) All connections of the internal network to external networks must be under the protection of a firewall. Demilitarized Zone (DMZ) networks require firewalls to protect their hosts from outside attacks, and their connections to other internal networks must have firewall protection.
3) Firewalls will be configured based on the level of risk imposed by the established connection.
4) Whenever resources are available, a risk assessment will be performed prior to introducing a new technology or application to the network.
5) Network access to an application containing critical or confidential data, and data sharing between applications, will be as authorized by the application owners and will require user authentication.
6) Information resources will be controlled to ensure access to network services, host services, and their subsystems are restricted to authorized users and uses only.
7) Authorization at network entry on the basis of valid user identification code and authentication (e.g., password) will be provided under the framework of network services and controlled by the network management program.
8) Network Administrators of wireless environments will change wireless vendor defaults, including default encryption keys, passwords, and Simple Network Management Protocol community strings, and ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.
9) Unless the ISM has provided a specific exception, passwords must be encrypted when transmitted across or stored on IT assets to prevent compromise.

10) While in transit, information which is confidential or information which in and of itself is sufficient to authorize disbursement of state funds will be encrypted.
11) Under no circumstance shall two networks be connected (this includes peer to peer traffic).
12) The establishment of any VPN allowing access to DEP's internal network requires written approval by the ISM and Network Administrator.

D. **Network Auditing**

1) The minimum requirements for audit logging of sensitive IT resources are:
   - Login with timestamp.
   - Source IP/Workstation Name.
2) OTIS will implement procedures to protect the integrity and confidentiality of audit logs.
3) OTIS will create, protect, and retain audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information and IT resource activity.
4) The agency ISM, Inspector General, Information Security Specialist or other specifically authorized personnel shall be granted access to review audit logs containing accountability details.
5) OTIS reserves the right to audit the use of all IT resources to ensure compliance with this Security Policy. Auditing of IT resources may include, but is not limited to, inspection of user access rights, examination of user access logs and electronic monitoring of user access by approved software tools.
6) Audit activity will be periodic and/or event driven to assure compliance with internal policies, support internal investigations, and assist the management of information systems.
7) System and security logs containing production IT resource security events will be retained for at least three months on a specified server and have limited access by only authorized personnel.
8) OTIS maintains tools and procedures to facilitate the monitoring of system activity.
9) The ISM or designee shall be provided access to monitor any agency IT resources.
10) Technology managers shall monitor technology resources to ensure desired performance and facilitate future capacity-based planning.

E. **Network Monitoring (Applies to all Computer Users/Workers)**

1) Employees suspected of misuse or violation may have their computer activity logged for further action and logs will be made available to management upon request.
2) To the extent that systems and software permit, all significant security related events will be logged. Examples of security related events may include User-ID switching during an online session, attempts to guess passwords, privilege escalation, and modification to production application software, system software or user privileges.
3) All employee accounts, workspaces and storage areas are subject to security reviews if the need arises. OTIS may review archived email, private file directories, hard disk drives, and other information stored on agency information systems.
4) Use of IT resources constitutes consent to monitoring activities whether a warning banner is displayed and acknowledged or not.
5) Monitoring, sniffing, and related security activities shall be performed only by Information Security or designee based on job duties and responsibilities.

6) OTIS will monitor for unauthorized IT resources connected to the agency network. Unauthorized access points connected to the agency network shall be removed immediately.

VI. APPLICATION SECURITY

OBJECTIVE

Computer security needs must be addressed as part of the Systems Development Lifecycle when developing new or making modifications to existing applications if the system or data affected by these applications must be protected from accidental or malicious access, use, modification, destruction, or disclosure. Furthermore, to adequately protect DEP information systems, OTIS will employ system development life cycle processes that incorporate information security considerations; employ software usage and installation restrictions; and ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

CONTROL

Appropriate security controls will be designed into applications to ensure correct processing of data. These controls will include validation of input data, internal processing and output of data, and adherence to strict coding guidelines as well as adherence to DEP's authentication and authorization protocols.

SCOPE AND POLICY

The Application Security Policy applies to all employees and anyone using agency IT resources. This policy has two sections: Application Security and Coding, Code Review, and Classification.

A. Application Security

1) Application developers will develop procedures to ensure application security is addressed throughout the application development lifecycle.
2) The application procurement/delivery process must ensure agreements and deliverables address application security requirements.
3) Application owners are responsible for defining application security-related business requirements.
4) The application development team shall implement appropriate security controls to achieve the security requirements of the application owner and implement appropriate security measures to minimize risks to agency IT resources.
5) OTIS will maintain procedures to establish accountability for accessing and modifying mission critical applications.
6) Any exceptions to standard security requirements and controls noted during development reviews will be assessed for approval by the ISM.
7) All software applications obtained, purchased, leased, or developed should provide appropriate security controls to minimize risks to the confidentiality, integrity, and availability of the application, its data, or other IT resources.
8) A sufficiently complete history of transactions shall be maintained for each session involving access to critical information to permit an audit of the system by tracing the activities of individuals through the system.
9) For third-party vendor applications that are implemented in production, the vendor must comply with contractually required security requirements.

B. **Coding, Code Review and Classification**

1) Developers should follow DEP approved coding standards, which provide for a consistent code base for developed applications.
2) Application developers must incorporate validation checks into applications to detect data corruption that may occur through processing errors or deliberate actions.
3) All applications will adhere to the Federal Information Processing Standards (FIPS) 199 categorization based on the criticalness to the agency's mission and service deliveries.
4) Source code is to be reviewed throughout the application development lifecycle for deficiencies in the areas of security, reliability, and operations.

VII. INFORMATION SYSTEMS CONTROLS

OBJECTIVE

Information System Controls is the policy section that provides the framework for configuration management and general security configuration practices designed to reduce IT security vulnerability. The Information Security Manager will periodically assess security controls to determine their effectiveness and appropriateness. Based on these assessments, the Information Security Manager will develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in information and IT resources.

CONTROL

Information systems include operating systems, infrastructure, applications, off-the-shelf products, services, and user-developed applications. The design and implementation of information systems supporting the agency can be critical for security. Security requirements, risk analysis and maintenance will be identified prior to the development and implementation of information systems.

SCOPE AND POLICY

The Information Development and Maintenance Policy extends to all workers and anyone using agency IT resources. This policy is broken up into the following sections: Security Configuration Requirements, Change Management, Encryption, Risk and Vulnerability Management and Maintenance.

A. Security Configuration Requirements for Information Systems

1) Specialized security controls, exceptions, and deviations from standard security configuration of an Information System must be documented in a way that is accessible to staff responsible for maintenance.
2) Service level agreements for technology services will be established when appropriate to ensure appropriate security controls are established and maintained.
3) IT resources and associated owners and custodians will be identified and documented.
4) Computing devices connecting to the agency network shall use current and up-to-date anti-virus software (where technology permits).
5) Agency computing devices shall activate an agency-approved personal firewall (where technology permits) when connected to a non-agency network.
6) DEP databases containing mission critical or confidential data shall be placed in an internal network zone, segregated from the DMZ.

B. Change Management

1) A change management process for modifications to production IT resources will be maintained.
2) Access to production IT resources for the purpose of troubleshooting, deploying code, or running ad hoc queries must be coordinated and scheduled to undergo the change management process.

3) Changes to production server applications must follow established change control procedures and must be completed by the appropriate personnel.
4) Design of ad hoc database queries that modify data in a production database must be approved and certified by DEP's Database Administrator before they can be used by any production IT resource. Controls shall be established to ensure the accuracy and completeness of data.
5) Changes to DEP's internal, business partner gateway, and Internet gateway networks, such as loading of a new router or switch, changing of network addresses, configuring routers or switches, or installing new network hardware or connectivity must follow establish change management processes.

C. **Encryption**

1) Data that is considered sensitive or vulnerable to unauthorized disclosure or modification during transmission or while in storage should be encrypted. Owners of sensitive information must analyze the risk and determine whether to use cryptographic protection following these guidelines.
2) Standard algorithms such as RSA (algorithm by Ron Rivest, Adi Shamir and Leonard Adleman) Advance Encryption Standard (AES), National Institute of Standards and Technology (Sha-2), Blowfish, Elliptic Curve Cryptography (ECC), and ElGamal and International Data Encryption Algorithm (IDEA) will be used as the basis for approved encryption technologies.
3) Encryption key lengths must be at least 128 bits or stronger.
4) The use of proprietary encryption algorithms is not allowed for any purpose, unless approved by the Information Security Manager.
5) OTIS will establish procedures to ensure agency cryptographic implementations are developed and maintained according to guidelines.
6) Key management processes and procedures for cryptographic keys used for encryption of confidential data will be fully documented and will cover key generation, distribution, storage, periodic changes, compromised key processes, prevention of unauthorized substitution.
7) Key management processes must be in place and verified prior to encrypting data at rest (including email messages, data files, hard drives, and data backups).
8) Sensitive information that is not encrypted will have appropriate security access controls in place to make sure only authorized users have access.

D. **Risk and Vulnerability Management**

1) Information Security will periodically assess the risk to agency operations (including mission, functions, image, or reputation), agency assets, and individuals, resulting from the operation of agency information and IT resources and the associated processing, storage, or transmission of agency information.
2) The ISM shall monitor and document IT risks and mitigation practices. An annual risk assessment will be provided to the CIO.
3) The ISM will ensure that risk mitigation plans to reduce identified risks to agency IT resources and data are properly implemented.
4) Documentation of the information security risk analysis and risk mitigation plans is confidential pursuant to Section 282.318, Florida Statutes, except that such information shall be available to the agency Inspector General and the Auditor General.

5) System Administrators, Application Owners and Database Administrators are responsible for the implementation of security procedures within their processes to protect agency information from loss, destruction, and unauthorized or improper modification.

E. **Maintenance**

1) System Administrators will perform periodic and timely maintenance on agency information and IT resources and shall provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information and IT resource maintenance.
2) IT resources are to be correctly maintained to ensure continued availability and integrity.
3) Administration of hardware, software, or applications performed over a network shall be encrypted where technology permits.
4) The application maintenance process shall include reviews of application security requirements and controls to ascertain effectiveness and appropriateness relative to new technologies and applicable state and federal regulations.
5) System Administrators will ensure all systems are at an acceptable patch and version level to protect the department's data and resources from risks related to compromised security controls.

VIII. INFORMATION SECURITY INCIDENT MANAGEMENT

OBJECTIVE

Formal event reporting and escalation procedures must be in place and all employees and contractors will be aware of these procedures for reporting the events and weaknesses that might have an impact on the security of DEP IT assets. All employees and contractors will be required to report any actual or suspected information security events (however minor in nature) and as quickly as possible to the Service Desk.

CONTROL

Information Security Incident Management Policy is established to ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken by the appropriate computer response personnel.

SCOPE AND POLICY

Information Security Incident Management Policy applies to all employees and anyone using agency IT resources. This policy is broken into the following section: Management of Information Security Incidents and Reporting.

A. **Reporting of Information Security Incidents (Applies to all Computer Users/Workers)**

1) Information Security must be notified of any suspected or confirmed computer security incidents, including suspected or confirmed breaches, within 24 hours of discovery.
2) Suspected computer security incidents shall be reported to the Service Desk at 850-245-7555 or call the ISM directly at the OTIS Reception Desk 850-245-8238.

B. **Management of Information Security Incidents and Reporting**

1) OTIS will maintain an operational Computer Security Incident Response Team (CSIRT) and document associated procedures to ensure adequate preparation, detection, analysis, containment, recovery, and response activities. The CSIRT will respond to suspected computer security incidents by identifying and controlling the incidents, notifying designated CSIRT responders, and reporting findings to agency management.
2) The CSIRT will track, document, and report incidents to appropriate agency officials, and other State and/or law enforcement authorities.
3) The CSIRT membership shall include at least one individual from the agency's legal, BHRM, inspector general, and IT areas, as well as the CIO and ISM.
4) The CSIRT under the direction of the CIO, Inspector General or ISM, shall determine the appropriate response required for each suspected computer security incident.
5) Computer security incident documentation is exempt from public disclosure, pursuant to Section 282.318, Florida Statutes.
6) The CSIRT shall convene at least once a quarter.
7) The CSIRT shall provide regular reports to the agency CIO.

8) Each suspected computer security incident, including findings and corrective actions, shall be documented, and maintained as specified in the agency computer security incident procedures. The computer security incident response process will include notification procedures to be followed for incidents where investigation determines non-encrypted personal information was, or is reasonably believed to have been, accessed by an unauthorized person, pursuant to Section 817.5681, Florida Statutes.

IX. BUSINESS CONTINUITY MANAGEMENT POLICY

OBJECTIVE

The Business Continuity Management Policy is the policy that establishes the standards for the protection of enterprise resources should a disaster strike. The purpose is to minimize the impact on DEP and recover from a loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and malicious actions) to an acceptable level through the combination of preventive and recovery controls. This policy will aide DEP to identify the critical agency business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transportation, and facilities.

CONTROL

To counteract interruption to DEP's activities and critical processes from the effect of major failures and/or disasters, OTIS will establish, maintain, implement, and test plans for backup/standby/redundant operations and disaster recovery of DEP information and IT resources to ensure the availability of critical IT resources and continuity of operations during emergency situations.

SCOPE AND POLICY

Understanding the risks DEP is facing in terms of probability and impact in time, including an identification and prioritization of critical processes, a managed level of service will be developed and maintained for business continuity throughout the agency and will apply to all employees and anyone using agency IT resources. This policy is broken up into the following sections: Business Continuity Management and Backup and Recovery.

A. Business Continuity Management

1) IT resources identified as critical to the continuity of governmental operations shall have documented disaster recovery plans to provide for the continuation of critical agency functions in the event of a disaster.
2) Information Technology Disaster Recovery Plans (ITDRP) shall be tested at least annually; results of the annual exercise shall document those plan procedures that were successful and what work is required to correct the plan.
3) All OTIS IT resources will be subject to a business impact analysis based on the consequences of disasters, security failures, loss of service and service availability.
4) Data and software essential to the continued operation of critical agency functions shall be mirrored to an off-site location or backed up regularly with a current copy stored at an off-site location.
5) All sensitive, valuable, or critical information that is resident on DEP computer systems and networks must be periodically backed up. System Administrators working with application owners must define which information should be backed up, the frequency of backups and the method of backups.
6) The agency shall ensure security controls over backup resources are appropriate to the criticality and confidentiality of the primary resources.

B. **Backup and Recovery (Applies to all Computer Users/Workers)**

1) To prevent loss of data, agency users shall ensure agency data stored on workstations or mobile devices is backed up. Options include OTIS maintained networked storage, OneDrive, SharePoint, or other OTIS approved backup solutions.
2) Backup and archival media must be stored at a separate location from the system being backed up.
3) External hard drives are not an appropriate mechanism for backing up system of record data or data that cannot be reproduced in a reasonably viable manner.

X. COMPLIANCE POLICY

OBJECTIVE
Compliance is the policy section that provides the context for the implementation and adherence of security policies and sets the framework and standards at DEP for monitoring by Information Security. If employees do not follow these policies and do not obtain an authorized exception, then violations and disciplinary action may occur.

CONTROL

The Compliance Policy was created to avoid breaches of any criminal or civil law, statutory, contractual obligation, and security requirements; to ensure compliance of the security policies and standards; and to maximize the effectiveness of these policies regarding Department IT resources.

SCOPE AND POLICY

The Compliance Policy applies to all employees and contractors and to anyone using agency IT resources. This policy contains two sections: Compliance and Exceptions to Security Policy.

A. **Compliance (Applies to all Computer Users/Workers)**

1) All employees and contractors must read, understand, and comply with this Information Security Policy.
2) Employees and contractors failing to comply with agency security policies and procedures are subject to disciplinary action appropriate to the violation up to and including termination and/or criminal prosecution.
3) Employees and contractors are responsible for complying with applicable state and federal security rules and laws.
4) Employees and contractors will agree, in writing, to comply with agency acceptable use policies prior to using agency IT resources.
5) Non-compliant employees, discovered in a routine Security Audit or in the course of work, may have their access privileges temporarily or permanently revoked.

B. **Exceptions to the Security Policies (Applies to all Computer Users/Workers)**

1) Limitations in resources and technical capabilities may prevent full compliance with some of the security requirements without introducing unacceptable business delays or work stoppage. When such cases arise, an Information Security Exception Request must be submitted for Information Security Manager (ISM) approval. Approved exceptions shall be maintained by the ISM and regularly reviewed. When an exception is no longer valid, the ISM shall revoke the exception and the requester must come into full compliance in a timely manner. If the agency cannot comply with a state information security policy, the ISM will coordinate with the Secretary to obtain the state's approval for an exception.
2) Personnel may not proceed with the exception until the ISM has confirmed in writing that the exception has been approved and has outlined any attached conditions.

DEFINITIONS

Access. The ability to acquire, read, write, or delete data or information; make use of an IT resource; enter a room or facility.

Access Control. The enforcement of specified authorization rules based on user or system authentication.

Access Point. A station that transmits and receives data (for example, a wireless access point).

Accountability. The principle stating that a specific action is traceable to a unique individual.

Administrator. A technical user responsible for administrating a multi-user system. Examples include System administrators, Network Administrators and Database administrators.

Agency-Approved Software. Software that has been reviewed and deemed acceptable by the agency for use with agency IT resources.

Agency managed device. A device that is not owned by the agency, but that is declared by the device owner and accepted by the agency to be compliant with agency standard configurations.

Agency Worker. see Worker.

Application. Information resources designed to satisfy a specific set of user requirements.

Application Development Team. The entire set of people responsible for planning, designing, developing, installing, and maintaining applications. The roles represented include project managers, analysts, computer programmers, database administrators, data administrators, system administrators, network administrators, etc.

Application Owner. The business unit that requested the application be developed and/or purchased; the individual (usually a manager) from the business unit(s) for which an application is acquired who has responsibility and authority to make decisions related to the application, such as requirements, deliverable approvals, access, etc.

Audit logs. Documentation of activity within a system incorporating, at a minimum, date, time, action, and user account associated with the action.

Authentication. The process of verifying that a user, process, or device is who or what it purports to be. Techniques for authentication, called factors, fall into categories as follows:

- Something the user knows, such as a password or PIN.
- Something the user has, such as a smartcard or ATM card.
- Something that is part of the user, such as a fingerprint, voice pattern or facial recognition.

Authorization. Official or legal permission or approval.

Availability. The principle that authorized users have timely and reliable access to information and IT resources.

Breach. Unlawful and/or unauthorized access of computerized data that materially compromises the security, confidentiality, or integrity of personal information.

Chief Information Officer (CIO). The person appointed by the agency head that coordinates and manages the agency IT functions and responsibilities.

Complex Password. A password that is at least twelve characters and is comprised of at least three of the following categories:

- Uppercase English letters.
- Lowercase English letters.
- Numbers 0-9.
- Non-alphanumeric, or special, characters.

Computer User. Any authorized entity that uses IT resources (interchangeable with User).

Confidential Information and/or Confidential Data. Information not subject to inspection by the public that may be released only to those persons and entities designated in Florida statute; information designated as confidential under provisions of federal law or rule.

Confidentiality. The principle that information is accessible only to those authorized.

Critical Information Resources. The resources determined by agency management to be essential to the agency's critical mission and functions, the loss of which would have severe or catastrophic adverse effects.

Cryptography. The discipline that embodies the principles and methods for the transformation of data in order to hide semantic content, prevent unauthorized use, or prevent undetected modification. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible, or "one way").

Custodian. An organizational unit that is the guardian or caretaker of an information resource that is charged with the resource owner's requirements for processing, telecommunications, protection controls, and output distribution for the resource. The custodian is normally a provider of services.

Data Catalog. The organized inventory of DEP data assets facilitated by the Data & Analytics Office.

Data store. A collection of information organized so it can be accessed, managed, and updated.

Degaussing. A method of bulk erasing data from magnetic media. Degaussing demagnetizes the disk such that all data stored on the disk is permanently destroyed.

Demilitarized Zone (DMZ). Physical or logical sub-network or computer host that provides an additional layer between the Internet and an organization's internal network so that external parties only have access to devices in the DMZ rather than the internal network.

Development Infrastructure. A technical environment that is used for design, development, and/or piloting of new technical capabilities or applications. The development infrastructure is separated logically or physically from the production and test infrastructures.

Directly Connect [to the agency internal network]. A device that is joined to and becomes an extension of the agency's internal network. Dial-up and Virtual Private Network (VPN) connections to the agency are considered to be directly connected.

Disaster Recovery Plan. See Information Technology Disaster Recovery Plan.

Encryption. The reversible process of transforming readable text into unreadable text (cipher text).

Exempt Information. Information an agency is not required to disclose under Section 119.07(1), Florida Statutes, but which the agency is not necessarily prohibited from disclosing in all circumstances.

Full format. Scans for bad sectors and writes zeros in all sectors, permanently deleting all data.

Hardware. Any physical device, equipment or external peripherals that enable users to perform agency functions such as input, output, storage, communication, processing, and more. These devices include but are not limited to computers, mobile devices such as laptops, phones, tablets; peripherals such as monitors, printers/scanners, keyboards, mice, and external storage devices.

Information Owner. The manager of the business unit ultimately responsible for the collection, maintenance, and dissemination of a specific collection of information.

Information Security. A specialized subset of OTIS employees charged with protecting information and IT resources from unauthorized access, use, disclosure, disruption, modification, or destruction. This includes the ISM as well as key Service Desk, and Systems personnel.

Information Security Manager (ISM). The person designated to administer the agency's information security program in accordance with Section 282.318, Florida Statutes.

Information Security Program. A coherent assembly of plans, project activities, and supporting resources contained within an administrative framework to assure adequate security for agency information and IT resources.

Information Technology Disaster Recovery Plan (ITDRP). IT resources and procedures to ensure the availability of critical resources needed to support the agency mission in the event of a disaster and to return to normal operations within an accepted timeframe. The ITDRP considers availability requirements, recovery time frames, recovery procedures, back-up/mirroring details, systematic and regular testing and

training.

Information Technology Infrastructure. Network devices, server hardware, and host operating systems, database management systems, utilities, and other assets required to deliver or support IT services. Information technology resources – a broad term that describes a set of technology related assets. While in some cases the term includes items such as people and maintenance, as used in this rule, this term means computer hardware, software, networks, devices, connections, applications, and data.

Information Technology Worker. An agency user whose job duties and responsibilities specify development, maintenance, or support of IT resources (see User; Worker; Workforce)

Integrity. The principle that assures information remains intact, correct, authentic, accurate and complete. Integrity involves preventing unauthorized and improper creation, modification, or destruction of information.

Interactive Session. A work session where there is an exchange of communication between a user and a computer.

Least Privilege. The principle that grants the minimum possible privileges to permit a legitimate action to enhance protection of data and functionality from faults and malicious behavior.

Malware. Malicious software: a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

Media. Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

Mobile Computing Device. A portable device that can process data (e.g., laptop, personal digital assistant, certain media players and cell phones).

Mobile Device. A general term describing both mobile computing and mobile storage devices.

Mobile Storage Device. Portable data storage media including external hard drives, thumb drives, floppy disks, recordable compact discs (CD-R/RW), recordable digital videodiscs (DVD-R/RW), or tape drives that may be easily attached to and detached from computing devices.

Multi-factor Authentication (MFA). A way of verifying your identity when you sign into a network, website, or application using two or more pieces of evidence, such as a password, a device, a code, or a biometric scan. MFA can help protect your accounts from unauthorized access.
Some examples of MFA are:

- Using a password and a code sent to your phone or email.
- Using a password and an app like Microsoft Authenticator.
- Using a password and a hardware key or a fingerprint scan.

National Institute of Standards and Technology (NIST). A non-regulatory Federal agency within the U.S. Department of Commerce's Technology Administration.

Need To Know. The principle that individuals are authorized to access only specific information needed to accomplish their individual job duties.

Network. An interconnected group of IT devices; a system that transmits any combination of voice, video and/or data between devices.

Operational Controls. Security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).

Owner. The manager of the business unit ultimately responsible for an IT resource.

Patch Management. The process for identifying, acquiring, testing, installing, and verifying software updates, also known as patches.

Peer to Peer. A communications model that allows the direct sharing of files (audio, video, data, and software) among computers.

Personal Firewall. Software installed on a computer or device which helps protect that system against unauthorized incoming or outgoing network traffic.

Personally Identifiable Information (PII). An individual's first name, first initial and last name, or any middle name and last name, in combination with any one or more of the following data elements:

- Social Security Number.
- Driver's license number or Florida Identification Card number.
- Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Note: as provided in Section 817.5681, Florida Statutes, the term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

Privately-Owned Device. A device not purchased with agency funds; a device owned by a person or other non-agency entity and not configured, maintained, or tracked by the agency.

Production Infrastructure. Network devices, server hardware, and host operating systems that comprise an agency's operational or real-time environment.

Quick format. Deletes the file system table and the root folder, freeing up space for other files. Does not permanently delete files.

Re-image. The process of restoring a computer or device to its original state by erasing the existing data and

configurations and reinstalling the operating system and essential software.

Remote Access. The ability for an authorized person to access a computer or network from a geographical distance through a network connection. Remote access is accomplished with a combination of software, hardware, and network connectivity.

Review. A formal or official examination of system records and activities that may be a separate agency prerogative or a part of a security audit.

Risk. The likelihood that a threat will occur and the potential impact of the threat.

Risk analysis. A process that systematically identifies valuable data, information, and IT system resources and threats to those resources, quantifies loss exposures (i.e., loss potential) based on estimated frequencies and costs of occurrence, and recommends how to allocate resources to countermeasures so as to minimize total exposure. The analysis lists risks in order of cost and criticality, thereby determining where countermeasures should be applied first. (To be used interchangeably with risk assessment.)

Risk management. The ongoing process of risk analysis and subsequent decisions and actions to accept risk or to reduce vulnerabilities by either mitigating the risks or applying cost effective controls.

Sanitize. A process to render access to target data on the media infeasible for a given level of effort. Clear, purge, damage, and destruct are actions that can be taken to sanitize media.

Security Controls. The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed to protect the confidentiality, integrity, and availability of IT resources.

Security Incident. Any action or activity, whether accidental or deliberate, that compromises the confidentiality, integrity, or availability of agency data or IT resources.

Security Review. An examination of system records and activities to determine the adequacy of system controls to ensure compliance with established security policy and operational procedures, detect breaches in security, and recommend any indicated changes in any of the foregoing.

Separation of Duties. The concept of having more than one person required to complete a task. This is a way to ensure that no one individual has the ability to control all critical stages of a process.

Service Account. An account used by a computer process and not by a human (e.g., an account used by the backup process for file access). Normally service accounts may not log on to a system.

Session. The time during which two devices maintain a connection and are usually engaged in transferring data or information.

Smart Card. A pocket-sized card with embedded circuits that can process data. Often smart cards are used

as a form of authentication for single sign-on systems (also known as integrated circuit card).

Sniffing. Capturing network data.

Software. Any set of instructions, programs, or statements and related data which, when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.

Special Trust or Position of Trust. Positions that, because of the special trust, responsibility, or sensitive location of those positions, require that persons occupying those positions be subject to a security background check, including fingerprinting, as a condition of employment, pursuant to F.S. Section 110.1127.

Standards. Specific set of practices or procedures to regulate how a system or organization provides services; required practices, controls, components, or configurations established by a recognized authority.

Standard Configuration. The documentation of the specific rules or settings used in setting up agency hardware, software, and operating systems.

Strategic Information Security Plan. The agency three-year plan that defines security goals, intermediate objectives, and projected agency costs for the strategic issues of information security policy, risk management, security training, security incident response, and survivability.

Strong Cryptography (encryption). Cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key-management practices. Secure Hash Algorithm revision 2 (SHA-2) is an example of an industry-tested and accepted hashing algorithm. Examples of industry-tested and accepted standards and algorithms for encryption include Advanced Encryption Standard (AES) 128 bits, Triple Data Encryption Standard (TDES), minimum double-length keys, Rivest, Shamir and Adleman (RSA), 1024 bits and higher, Elliptic Curve Cryptography (ECC), 160 bits and higher, and ElGamal (1024 bits and higher).

Survivability. The capability of an organization to maintain or quickly recover critical business functions after a disaster or adverse event, minimize the effect of an event, reduce financial loss, and expedite the return to normalcy.

System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, storing, reporting, printing, dissemination, or disposition of information.

System Administrator. A person in charge of managing and maintaining computer or telecommunication systems.

Systems Development Life Cycle (SDLC). A set of procedures to guide the development and modification of production application software and data items. A typical SDLC includes design, development, quality assurance, acceptance testing, maintenance, and disposal.

Technical Controls. Security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the

hardware, software, or firmware components of the system.

Test Infrastructure. A technical environment that mirrors part or the entire production environment and is used for final testing of a technology or an application prior to production implementation. The test infrastructure is separated logically or physically from the production and development infrastructure.

Track. The documented assignment of an asset to a user and/or location.

User. Any authorized entity that uses IT resources (see Worker; Workforce; Information Technology Worker).

Virtual Private Network (VPN). A secure encrypted connection over the Internet from a device to a network.

Warning Banner. A message displayed prior to or upon connection to a resource informing the user that activities may be monitored, or access is restricted.

Worker. A member of the workforce that may or may not use IT resources (see User; Workforce; Information Technology Worker).

Workforce. Employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, is under the direct control of the agency, whether or not they are paid by the agency (see User; Worker; Information Technology Worker).

Administrative Directive
DEP 375

Approved by the Secretary
Effective 5-3-2024

Records Management and Public Records Access

RECORDS MANAGEMENT

RETAINING, PRESERVING, AND DISPOSING OF PUBLIC RECORDS

Roles & Responsibilities

The Florida Department of Environmental Protection (DEP) is committed to preserving and retaining records in accordance with Florida law, Directives, policies and procedures, and Department of State (DOS) policies. The Office of the Ombudsman and Public Services is responsible for processing and reporting Records Deposition Requests and updating the department's Records Retention Schedule.

1. **Records Management Liaison Officer.** The Ombudsman shall designate a member of the Ombudsman's Office to serve as the Department's *Records Management Liaison Officer (RMLO)* to assist the Ombudsman in carrying out the following responsibilities:
   - Serving as the official point of contact between the Department and DOS Division of Library and Information Services records management program.
   - Complying with and submitting reports that may be required by the DOS, Executive Office of the Governor, or by law.
   - Approving and rescinding Records Retention Liaison's (RRL) access to the DOS's Total Recall Records Management System (TRRMS).
   - Working with Districts/Divisions/Offices to maintain and update retention schedules.
   - Consulting and advising on DEP record inventories, disposition of existing records, and development of procedures for appropriate disposal of records that have reached their retention limit.
   - Advising and making recommendations to leadership on best practices, policy needs, and procedural improvements related to records managements and retention.
   - Managing the department's RRL's to ensure they have, information, tools, and resources needed to support the departments records disposition processes.
   - Developing content and implement a schedule for regular training of new employees, current staff, and RRL.
   - Working with the General Counsel and other internal stake holders on Departmental policy.
   - Responding to questions from external customers regarding agency records.

2. **Records Retention Liaisons.** Each major department sub-division (district/division/office/area of responsibility) shall appoint an RRL within that sub-division. This RRL is solely selected and approved by division director at their discretion and submitted to the RMLO to add to the master RRL list. The RRL is responsible for the records retention and disposal process within their sub-division.[1] The RRL's responsibilities include:

   - Ensuring the RRL's divisional unit's leadership and staff are aware of records retention requirements and facilitating compliance efforts.

[1] Each District/Division/Office with a Records Liaison's Division Director may also nominate an Assistant Records Retention Liaison (ARRL).

- Advising divisional unit on the storage, labeling, and indexing of records in an organized way so they are secure and accessible, including vital, permanent or archival records.
- Ensuring all the division unit's managed records have an approved retention schedule and working with the RMLO to establish schedules for new categories of records.
- Regularly reviewing local retention schedules and advising the RMLO when items should be updated.
- Consulting and advising on record inventories and the disposition of existing records within their area of responsibility.
- Coordinating with the RMLO, and other Retention Liaisons as necessary to raise awareness of any training, support, information, tools, and resources needed to succeed.
- Assisting the RMLO with compiling any reports by providing requested information in a timely manner.
- Responding to questions from external customers regarding locally stored records.
- Following established procedures and facilitating the appropriate disposal of records that have reached their retention limit.

3. **Retention.** Unless otherwise required,[2] all records in Department custody must be retained and stored by the agency for the full period of their established retention schedule as set forth in the Retention Schedule set by the DOS (GS1-SL). If the DOS schedule does not apply, the record shall be retained in accordance with DEP's Retention Schedule available at: https://www.floridadep.net/resources/records-retention-and-disposition.

4. **Storage**

- **General.** When determining how to store records (e.g., paper, digital, video, film, etc.), staff should consider the life expectancy of the record (not the content and context of the record). The natural deterioration rate for that platform must be considered to ensure that it will remain legible for the entirety of its retention period. If records are being stored on platforms that are not expected to reach the required retention date, the records' owner must work with subject matter leadership and the RRL to establish a plan to update the platform at an appropriate date in the future. For example, VHS videotape deteriorates 10 to 20 percent over the course of 10 to 25 years; thus, any the retention schedules should be reviewed for all records stored in that format to ensure they do not have to be retained longer than 10 years. If they do, a future format transfer should be planned.

  Another consideration in deciding how to store records is accessibility. All records must be accessible. For example, if there are records stored on VHS, there must be a working VHS machine available to play the tape.

- **Physical Storage.** Precautions should be taken to ensure records are not stored in areas or manners that may lead to their damage or premature destruction. Records should be kept in secure areas with appropriate climates, facilities, access, and cataloging to ensure they are maintained throughout their retention periods. For example, paper should be stored in cool, clean, low humidity, low light, environments with appropriate air flow. And no paper documents should be stored where they are exposed to dripping pipes, bright lights, and exposure to rodents or insects.

[2] In some cases, records are legally required to be retained beyond their regular retention schedule (e.g., records under audit, records pending a public records request, and records related to a pending or impending legal action).

- **Electronic Storage**
  - **Email.** Department emails are automatically deleted every five years. As such, all emails remaining in the system at the five-year point must fall into either the "duplicate copies" or "administrative convenience" retention schedules.

    The agency email system may not be used as a storage format for documents. Emails and attachments that are pertinent to issues with extended retention schedules must be saved into appropriate formats for longer-term storage and cataloging. Individual staff is responsible for policing their email to ensure records are appropriately saved, transferred, cataloged, and stored.

  - **Total Recall Records Management System**. The Florida Department of State's TRRMS allows State Agencies to manage their records online. Users may upload records into the Records Center, submit work orders to retrieve, refile, or permanently withdraw their records as well as order supplies such as boxes, barcodes, and labels. The RMLO is authorized to grant and rescind access to TRRMS as appropriate. The RMLO shall ensure that RRLs have appropriate training and knowledge before authorizing access to TRRMS. Once authorized, RRLs shall manage the TRRMS according to DOS's guidelines. All Retention Schedule Requests and TRRMS Access Requests must be routed to the RMLO for approval prior to transmittal to the DOS.

5. **Conversion and Copying.** If the need arises to transfer records from one media to another (e.g., paper to electronic), and thereby create a new copy of a record *before* they have reached the end of their retention requirements:

   - Divisions/Districts/Offices must ensure that the receiving media (where the new copy of record will be stored) conforms to standards set forth in Rule 1B-26.003, F.A.C.
   - Quality Assurance (QA) must be conducted to ensure that the content of all transferred records is visible and legible in their entirety, all data is captured, and the document is correctly indexed in the new format. QA is complete when a second person has verified the record is in the approved converted format, is at least as legible as the original, contains all data information, and is correctly indexed.
   - Hard copies of *PERMANENT* records may only be destroyed AFTER they are converted to another approved media (i.e., electronic imaging), thorough QA review of the new version is completed to ensure all record data from the originals is saved in accordance with Rule 1B-26.0021, F.A.C., AND approval has been received from the RMLO.
   - Conversion of new and current records may be done in the daily course of business. No extra reporting or permission is required. Retroactive Conversion (bulk and historical transfer projects) must be submitted to the RMLO through Records Disposition Request, via the designated system, and the RMLO must provide approval before the original record may be disposed of per Rule 1B-24.001(3)(m), F.A.C.

6. **Disposition**

   - **Timing.** Records shall be disposed of in accordance with the GS1-SL and DEP Retention Schedules and following the disposition process. Records shall only be retained beyond their retention schedule in the following situations:

- An audit is either pending or in progress.
- Legal action or litigation is in progress.
- A public records request for the records was received within the last 30 days.
- A federal or state law or DEP rule requires retention or prohibits destruction.
- Subject matter leadership has determined it still has significant value to ongoing official business.

The RRL is required to check for the above listed contingencies before requesting the disposition of a record.

- **Internal Procedure.** Records that have a retention schedule of "obsolete, superseded, or lost administrative value" may be disposed at the direction of leadership within any given divisional unit. All other records must be disposed of as follows:
  - When a record is ready for disposition, the RRL or ARRL shall complete and submit the Records Disposition Request, which may be filed up to ninety (90) days before the anticipated destruction date, so long as the actual destruction date is past the retention schedule.
  - The RRL must review and verify all records that are sought to be disposed of within the RRL's respective divisional unit to verify the record is eligible for disposition under the applicable retention schedule and does not fall within one of the above contingencies to be retained beyond disposition. Upon this verification, the RRL must forward the Disposition Form to the RMLO.
  - When a disposition form is submitted, the RMLO must review it and make a final determination of eligibility for disposition.
  - Upon RMLO approval and pursuant to Rule 1B-24.001(3)(m), F.A.C, records destruction should be carried out by the requestor as expeditiously as possible.
    - ✓ The DEP employee requesting disposition shall destroy the records in a manner that appropriately safeguards the safety, security, and privacy of individuals, private organizations, and the State of Florida whose data they may contain.
    - ✓ Destruction of records with designations of heightened security (sensitive, classified, trade secret, etc.) must be dispositioned according to DOS guidelines.
  - Once destruction/disposition is completed, the DEP employee who destroyed the record must return the Records Disposition Request, and enter the date of destruction via the system available at: https://www.floridadep.net/resources/public-records-request.
  - Completed Records Disposition Request will be cataloged and saved in the designated electronic document storage system according to their schedule guidelines.

- **Electronic Documents.** Requests to delete records from any Electronic Document Management System (EDMS) should be submitted using Records Disposition Request (as described above). No records will be deleted from the EDMS without prior approval from the RMLO and following DEP's disposition process described above. Only Division OCULUS Administrators may delete records from the EDMS and only after approval from the RMLO following the disposition process. Refer to DEP 390, Information Technology Resource Security and ADM 371, Electronic Document Management System, for more information on granting access or being granted access to electronic documents in the EDMS. New and current documents inserted into the EDMS in error may be deleted or moved to the appropriate catalog location by the Division's designee without submitting a Records Disposition Form.

- **Archival Documents.** Some records have enduring historical, administrative, or fiscal value. When this is known at the time that they are created, the records should be marked and included in a records series with this designation. However, the historical value is not always known when records are created. RRLs should review records for historical significance before disposition. Questions about historical value should be presented to and considered by subject matter leadership. Should subject matter leadership be unable to determine if records have historical value, they should contact the RMLO, who will coordinate a discussion with appropriate department leadership and the state archives.

  The characteristics of records that justify their continued retention as archives include values such as:
  - Evidential. They provide important value in explaining the agency's origins, structure, functions, and operations.
  - Informational. They provide important research or reference value.
  - Financial, legal, and administrative. They provide important information needed to conduct current and/or future agency business.
  - Intrinsic. The records are associated with an important historical event, structure, person, group of people, or in their unique physical format.

  For more information on the designation of historical documents for the state archives, refer to the current Florida Department of State "Basics of Records Management" Handbook, which can be found here: https://dos.myflorida.com/library-archives/records-management/forms-and-publications/.

  The State Archives of Florida, a program of the Division of Library and Information Services, serves as the central repository for the archives of state government. The State Archives of Florida analyzes record series to identify records having enduring historic, administrative, or fiscal value that may be eligible for permanent preservation. This criteria is explained in the GS1-SL for State and Local Government Agencies (https://dos.myflorida.com/library-archives/records-management/general-records-schedules) and should be considered in the disposal or preservation records. If a record series description states, "These records may have archival value," the RRL must contact the RMLO for archival review before the disposition of the records. The State Archives will provide guidance for the transfer of the records to the State Archives or other appropriate disposition of the records. For records indicating both permanent retention and possible archival value, the RRL should contact the RMLO after five years for archival review and guidance as to whether, when, and how to transfer the records to the State Archives.

- **Accident or Disaster.** Records that are unintentionally lost or destroyed by accident or disaster (theft, negligence, fire, flood, etc.) should be recorded using the records disposition process as described above.

PUBLIC RECORDS ACCESS

Roles & Responsibilities

The Department is committed to the letter and spirit of the Public Records Act (Chapter 119, Florida Statutes). This Act governs the public's right to inspect and obtain copies of records held by state and local governmental bodies. The Department's Office of the Ombudsman and Public Services, in coordination with the General Counsel, will (1) facilitate Floridian's right to access the public records of the Department; (2) provide information on readily requesting public records; and (3) provide routine training for Department officials and employees regarding Florida's public records and sunshine laws.

1. Public Records Liaison Officer

The Ombudsman shall designate a member of the Ombudsman's Office to serve as the Department's *Public Records Liaison Officer (PRLO)* and assist the Ombudsman in carrying out the following responsibilities:

- Receiving and responding to records requests from the public.
- Developing and implementing standard Department-wide policies, procedures, and systems for records retention and records request issues in compliance with applicable laws and directives.
- Establishing and managing a network of statewide liaisons within each distinct Department division, office, or district who will act as the public records liaison (PRL) and point of contact within their areas of responsibility.
- Continually improving and ensuring continuity of policies, procedures, and instructional content for training.
- Coordinating with Office of Organizational Development and Engagement to implement a schedule for regular training of new employees, current staff, and liaisons.
- Developing and managing systems to efficiently process, track, report, and conduct analytics on activities and outcomes related to public records and requests for public records.
- Working with and include input from the General Counsel and other internal stakeholders, as necessary to facilitate department responses to records requests.
- Advising and making recommendations to senior leadership on best practices, policies, and procedural improvements regarding public records and requests for public records.
- Providing information and respond to questions concerning public records from internal and external customers.

2. Public Records Liaisons

Each division/district/office of responsibility leadership must appoint a *PRL*.[3] PRLs will serve as "case assignees" for public records issues and have the following responsibilities acting as the central and exclusive point of contact for facilitating, tracking, and responding to records requests assigned within their area of responsibility.

- Coordinating with the requesters to ensure requests are properly fulfilled.

[3] Multiple offices within the Department may, at their own discretion, choose to have an individual serve as a Public Records Liaison, but that multiple-office liaison must be able to carry out all the required duties and responsibilities of an individual office's liaison. Additionally, an office may create assistant Public Records Liaisons.

- Providing status updates to requesters.
- Invoicing and collection from requesters.
- Establishing processes within their areas of responsibility for collecting, reviewing, and providing public records in accordance with DEP protocols.
- Coordinating with the Office of the Ombudsman and Public Services and other PRL's.
  - Assisting the Office of the Ombudsman and Public Services with compiling any reports and data, by providing the requested information in a timely manner.
  - Coordinating with the Office of the General Counsel for all legal questions concerning public records requests.

3. Processing Public Records Requests

Responding to public records requests is a duty and responsibility of all DEP staff. Chapter 119, Florida Statutes does not contain a specific time limit for fulfilling a public records request, but the courts have said that requests should be fulfilled within a reasonable time period. This means that it must be scheduled as an activity requiring prompt review and response. Staff is not required to immediately stop all previously scheduled, or in-progress work to address the request, but they must make its fulfillment a priority as they plan out their short-term schedule. All public records requests should be taken seriously by all DEP staff. There are personal and department penalties for deliberately or fraudulently not providing responsive records and for not providing records within a reasonable time.

- **Acceptance, Acknowledgment, & Assignment.** Public records requests shall be accepted during regular business hours. Requests delivered outside of business hours will be processed as received on the next regular business day. Individuals requesting public records are not required to provide their identity, address, affiliation, or the purpose for requesting the records.

  Any DEP employee, contractor or agent who receives a public records request must immediately forward the request to the Public Record Liaison within the employee/contractor/agent who is assigned to their office so that the request can be entered into DEP's online tracking system. The PRL must (1) immediately acknowledge the request and (2) log the request into the system within two days of receipt. The acknowledgement should advise the requestor that their request was received, it will be reviewed, and that there may be charges should it require extensive labor or resources to fulfill. It should not confirm whether such records exist.

  It is the ultimate responsibility of the employee/contractor/agent who received the request and the PRL to confirm that the request was timely acknowledged and logged into the system. This responsibility applies even if the request is unrelated to the employee/contractor/agent's division, district, office, or job specialty.

  Once a public records request is submitted into the system, it will automatically create a "case" with a digital record of when it was submitted. Each case file includes the text (or transcript) of the original request, contact information for the requestor and any attached correspondence. Each case also has a unique number to facilitate tracking, alerts, and analytics.

  The Office of the Ombudsman and Public Services will ensure all necessary information is provided, conduct any quality control needed and then determine to which district/division/office it should be

assigned. The Office of the Ombudsman and Public Services will assign the case (along with all pertinent details, contact information, and deadlines) to the PRL(s) within the most appropriate District/Division/Office.

When assigning the case to the appropriate liaisons, the Ombudsman will also copy (a) the OGC public records attorney when the request involves potential or pending litigation or is made by a law office or attorney; (b) the Office of Legislative Affairs Director when the request comes from an elected official of staff thereto; and (c) the Press Secretary when the request relates to potential or ongoing media issues or is made by a reporter or staff thereto.

- **Record Identification & Retrieval.** Upon case assignment, the assigned PRLs are responsible for coordinating the search for records starting within their own areas of responsibility and locating the requested records. The processes by which to identify and retrieve such records may vary depending on the structure of the PRL' areas of responsibility. The PRL must work with their managers to develop and oversee the process that works most efficiently within their areas of responsibility.

- **Defining Scope.** Requesters are expected to frame their requests in a clear and concise manner so that staff are able to reasonably determine which records are sought. If the scope of the request is unclear, the PRLs should contact the requester to better identify exactly which records are sought. While there is certain information the requester is not required to provide; they must be able to clearly identify the desired records or their search parameters. PRLs may assist the requester with the process but are not required to pursue or research records based on vague or unclear parameters.

  When the scope of a request is overly broad, vague, unclear, or incomplete (i.e., asks for "all water communications" or "all leadership emails," etc.) PRLs may ask the requester to clarify the search parameters including date ranges, keywords, email addresses, etc. to begin the search process. When necessary, the PRL may ask the requestor for additional information or to clarify details in order to process the request. If requestors refuse to provide necessary such parameters, which they are entitled to do, and there is not enough information to process a search, PRLs may advise them that the search cannot be conducted or that extensive use charges will be required to continue (see section 3 on cost estimates).

- **Identifying Electronically Stored Documents.** As soon as email search terms and date range are established, the PRLs should promptly email the information to the to the Office of Technology and Information Services (OTIS) Service Desk for processing. After running the search, OTIS will respond with the number of emails that were retrieved.

  Personal emails, voicemails, text messages, instant messaging, and all other electronic means of communication that relate to state business and responsive to a request are public records. Similarly, there may be responsive electronically stored documents that are not communications but are being held to formulate and perpetuate knowledge. Such documents are public records regardless of where such documents are stored – e.g., personal devices, in the cloud, etc. PRLs must work with the employees within their area of responsibility and PRLO to identify such documents. OGC should be

consulted concerning any questions as to whether such documents are public records under the Public Records Act.

When records are requested that are stored in a database, PRLs should work closely with the administrators of the database to identify the requested documents.

- **Internal DEP Coordination.** When cases involve research and collection of a large number of records, multiple divisions and subject matter areas, the Office of the Ombudsman will assign multiple PRLs. The PRLs should remain in communication with one another and the PRLO while their respective searches are ongoing. The PRLO shall serve as the lead coordinator and provide a central file to store and review records as they are retrieved and take the lead on the remaining steps in the process in place of the liaison.

  Liaisons shall coordinate with and consult the following offices under the specified circumstances:

  - ✓ The **Office of General Counsel** should be advised of requests relating to potential or ongoing legal issues. This includes but is not limited to all requests from a law firm, attorneys, legal support staff, or general counsels' offices.
  - ✓ The **Press Office** should be advised of requests relating to potential or ongoing media issues. This includes but is not limited to reporters or other members of the media.
  - ✓ The **Office of Public Services** should be advised of requests relating to potential or ongoing advocacy campaigns by citizens or groups.
  - ✓ The **Office of Legislative Affairs** should be advised when the request comes from an elected official or staff.

  Each PRL is responsible for communicating any public records requests to their Division/Office/ District director that may be of heightened agency concern. The Division/Office/District director shall review these public record requests prior to fulfillment. This includes matters that may be of a controversial nature, significant public interest, or involve leadership in DEP or other governmental agency/office. This communication and review should in no way delay or hinder the fulfillment of a public records request.

- **Provide Cost Estimate.** If, after determining the scope and identifying the records requested, it is apparent it will take more than 30 minutes of staff time to gather, review and redact the records, then charges should be assessed. The PRLs (or PRLO, when the lead coordinator) must estimate the costs in accordance with the following guidelines:

  - ➢ Labor costs must be based on the actual cost incurred (staff hourly salary plus benefits) by DEP in fulfilling the request. For purposes of calculating the actual costs, the appropriate Budget Coordinator for the employee's Division/District/Office may be contacted to attain the cost to the Department. When possible, records requests should be completed by staff with the lowest costs to DEP and the public. PRL must know or know where to find these staffing costs, and to track them.
  - ➢ Data Processing Charges may be applied if OTIS computer systems are required to locate records. Contact the OTIS Service Desk for assistance with coordinating logistics, usage,

and a determination of costs. There is generally no charge for the use of office desktop or personal type computers.

- All packaging, postage, and shipping costs incurred in the delivery of records should be charged to the requester.
- The following costs for duplication, copying, and supplies are determined by Chapter 119, Florida Statute, and may not be exceeded.
- No state sales tax will be charged in assessing the special service charge associated with public records requests.

Supply	Description	Unit Cost
Single-sided	Up to 8 ½ x 14 inches	$0.15 per sheet
Double-sided	Up to 8 ½ x 14 inches	$0.20 per sheet
CD-ROM	Disc with sleeve	$0.85 each
DVD	Disc with sleeve	$1.15 each
Certified Copy	N/A	$1.00 per record

After assessing the anticipated cost, the PRL (or PRLO, when the lead coordinator) must then contact the requestor and provide them with a detailed cost estimate. The requester must then agree to the costs, narrow the request, or withdraw the request. Where substantial costs will be incurred, an advance deposit of 75 percent of the estimate total shall be collected before beginning the next step of the process.

- **Record Review.** Under the Public Records Act, DEP must protect information defined as confidential or otherwise prohibited from public inspection or copying. Accordingly, each area of responsibility within the Department must review all requested and retrieved records for confidential and exempt information. The PRL over such areas are responsible for directing the review. Legal questions regarding the Public Records Act's exemptions and confidentiality provisions should be directed to OGC.

  When confidential or exempt information is discovered, the record must be redacted before supplying the document to the requestor or, if the entire record is confidential or exempt, the record should be withheld from disclosure. If any records are required to be redacted or withheld, the assignee must develop a redaction log, which will be provided to the requestor. A redaction log list is required that include responsive records not provided, the type of record redacted, and the statutory exemption that directs they be excluded from public release.

  As specified above, OTIS is responsible for locating emails that are responsive to public records requests pursuant to search terms established by the requestor or, if the requestor refuses, the PRLs within the area of responsibility for the request. Once the emails are located, OTIS will provide access to the emails to the PRL and the reviewers within the PRL's area of responsibility so that they can be reviewed for confidential and exempt information.

- Providing Records. After the records have been reviewed, the liaisons should prepare a final invoice that details the costs incurred (in accordance with II.A.3. above) and explain payment procedures. Payment is due at the time that the requester is provided with an invoice. No records shall be provided until the requester has paid the invoice in full. When deposits and payments are received,

they must be logged into the designated public records tracking system available at https://www.floridadep.net/resources/public-records-request. For specific steps on how to use this software, contact the PRLO for more information on this process and the next steps.

Upon payment in full, copies of the requested records and redaction log (if applicable) should be provided to the requester in the most cost-effective manner available to DEP while considering the needs of the requester. Whichever manner is chosen, DEP has an obligation to preserve the integrity of public records and prevent modification or destruction of original records. Such manners of providing records include:

- **Electronic Inspection.** Inspections can often be conducted electronically by using web-based platforms. Liaisons are encouraged to use such platforms when authorized and available. This includes but is not limited to publicly accessible online databases, such as DEP OCULUS, DEP FTP sites, online drop boxes, and the sharing of links via email.

- **Sending Copies (Electronically or Physically)**. Records can often be copied or scanned by the department and sent to the requestor electronically (e.g., email attachments) or physically (e.g., thumb drives or paper copies). After copies are made the original records shall be returned to their original location.

- **Physical Inspection**. In rare cases, it is more efficient for the requestor to come to a DEP office building to and physically inspect and/or copy the requested records. This includes inspecting the original hard files, electronic files or copies thereof. For example, the request might involve the inspection of a DEP database, historic state land maps in the State Lands Section Archives or geological reports at the Florida Geological Survey Office. In every situation, the physical inspection and copying of original records must be done under supervision of the public records' custodian or their designee. If the requestor seeks to photograph or photocopy the records being inspected, the intent to do so should be known in advanced so that the logistics can be coordinated, and DEP staff can ensure the records being copied are conducive to the copying method being used.

  DEP is not required to change the format of records. However, this may be done at the custodian's discretion to access the most cost-effective and efficient delivery tool. Formatting for Metadata requests related to electronic records must be coordinated with OTIS.

  Copies of submitted records should not be retained unless it is anticipated that there will be additional use for the copied records within the next year.

- **Closing Completed Public Records Requests.** Prior to closing the case, liaisons must ensure:
  - The above process was adequately followed;
  - All instructions on the case assignment were followed;
  - Due diligence and good faith efforts were made to provide all records responsive to the request; and
  - All outstanding payments for costs have been received and logged.

After verifying these requirements, the PRL shall ensure the case is closed as completed, designating that no further action is required. Contact the PRLO for more information on steps in this process and how to close out a case in the appropriate tracking systems and software.

If legal questions arise at any point in the above process, contact the Office of General Counsel public records attorney. Non-legal and logistical questions shall be referred to the Ombudsman's office.

AUTHORITY

This directive governs the Department's internal process for retaining, preserving, and disposing of public records and providing access to public records in accordance with:

Public Records, Chapter 119, Florida Statutes
Public Libraries and State Archives, Chapter 257, Florida Statutes
Public Records Scheduling and Disposition, Chapter 1B-24, Florida Administrative Code
Records Management - Standards and Requirements, Chapter 1B-26, Florida Administrative Code

Administrative Directive
DEP 420

Effective October 27, 2025

Drug-Free Workplace and Drug Testing

This directive states policy and establishes procedures for the implementation and administration of drug testing employees and maintaining a drug-free workplace within the Department of Environmental Protection (DEP).

AUTHORITY

Department of Law Enforcement, Chapter 943, Florida Statutes
Drug-Free Workplace Act, Section 112.0455, Florida Statutes
Drug-Free Workplace Program Requirements, Section 440.102, Florida Statutes
Drug-Free Workplace Standards, Chapter 59A-24, Florida Administrative Code
Drug Abuse Prevention and Control, Section 893.02, Florida Statutes
Controlled Substances and Alcohol Use and Testing, Federal Regulation 49 CFR 382
Grievance Procedures, Section 447.0401, Florida Statutes
Suspensions, Dismissals, Reductions in Pay, Demotions, Layoffs, Transfers, and Grievances, Section 110.227, Florida Statutes
Transportation, Federal Regulation Title 49 CFR

OVERVIEW

It is the policy of the department to ensure a drug-free workplace in compliance with federal and state laws. DEP's Drug-Free Workplace and Drug Testing directive is part of the effort to ensure that employees are performing efficiently and without undue risk to themselves or to the citizens of this state. This directive is to further ensure management complies with drug testing procedures and that all employees are aware that use or possession of illegal drugs or alcohol at the workplace is prohibited and may result in disciplinary action up to and including dismissal.

The department prohibits the unlawful manufacture, distribution, dispensing, possession, use of or being under the influence of a drug, as defined in this directive, in any DEP work location, by any DEP employee while on duty, state property, including operating or riding as a passenger on or in state-owned equipment; whether on or off duty, and while traveling in duty status on state business.

The abuse of alcohol or controlled substances is inconsistent with the behavior expected of employees, subjects all employees and the public to unacceptable safety risks and undermines the department's ability to operate effectively and efficiently. Further, the abuse of alcohol or controlled substances or the unlawful manufacture, distribution, dispensation, possession, sale or use of a controlled substance in the workplace while engaged in the department's business is strictly prohibited. Such conduct is also prohibited during non-working hours to the extent that it impairs an employee's credibility or ability to perform on the job or threatens the reputation, or integrity of the department. Off-duty employees are subject to the provisions of this directive and DEP 435, Conduct of Employees Directive when such activity constitutes a violation of federal, state or agency laws, rules, regulations, directives, general orders, operating procedures and/or standards of conduct.

An applicant or employee who refuses to submit to a drug test authorized by the department will be considered to have violated this directive and will be denied employment or be subject to disciplinary action, up to and including dismissal. Any instance of illegal drug use by a sworn law enforcement employee, an employee in a safety-sensitive position, or a commercial driver license (CDL) designated position is considered, in itself, to interfere with job performance. An employee in a CDL designated position whom refuses to submit to such tests shall not be permitted to drive or continue to perform safety-sensitive functions per Title 49 Part 382.211 CFR.

This directive applies to all department employees including part-time and OPS employees, and contracted drivers when they are on DEP property or when performing job related activities or business. This directive also applies to off-site or break periods when the individual (employee or contracted driver) is scheduled to return to work.

Nothing in this directive shall be construed to prevent DEP from establishing reasonable work rules or alter existing standards of conduct related to employee possession, use, sale or solicitation of drugs, including convictions for drug-related offenses, and from taking action based upon a violation of such rules or standards of conduct, in the absence of drug testing.

DRUG TESTING

The Bureau of Human Resource Management (BHRM) serves as the coordinating office for the drug testing program and will ensure each employee has access to a copy of this directive, maintain acknowledgment receipts, ensure applicable job announcements contain information relating to drug and alcohol testing, coordinate the selection of the drug and alcohol testing vendor, maintain and receive drug test results. All new employees will receive and acknowledge receipt of this directive when they are initially hired. All employees will have 24/7 access to this directive via the intranet. Drugs authorized to be tested for under this directive are as listed in Section 112.0455, F.S. (Drug-Free Workplace Act).

Drug Testing authorized under this directive are listed below as defined in Federal Highway Administration Rule 49 CFR 382. The following tests are regulated and collected/processed in accordance with section 49 CFR 40.71.

Pre-Employment. An applicant, including any current employee, for initial appointment to a position designated as a sworn law enforcement position, or a CDL designated position will be required to pass the appropriate controlled substance (drug) test. It will be the employing division's responsibility to schedule the appropriate drug test through BHRM after the applicant has been selected and approved for a contingent offer.

Post-Accident Test. An employee in a CDL designated position will be drug tested when involved in an accident with a commercial motor vehicle resulting in a citation or loss of human life.

Random Test. An employee in a CDL designated position will be randomly selected to conduct a drug test as required by law. The agency must, at a minimum, randomly test 10 percent of the average number

of CDL positions for alcohol and 50 percent for drugs. The selected employee will be notified by their designated division personnel to report to the nearest drug testing facility in their work area.

Reasonable Suspicion. Any department employee will be required to submit to a drug test when it is believed that the employee is using or has used drugs or alcohol in violation of this directive. Reasonable suspicion drug testing will not be conducted except upon the recommendation of a supervisor who is at least one level of supervision higher than the immediate supervisor of the employee in question. Reasonable suspicion may be based upon such facts and inferences as listed on DEP 54-105, Reasonable Suspicion Observation Form and as outlined below. This checklist must be prepared and signed and submitted to HR_ER@FloridaDEP.gov within 24 hours of the observed behavior when an employee is suspected of drug or alcohol use.

When it is determined that an employee meets more than one of the following categories for reasonable suspicion drug testing, the supervisor shall consult with a supervisor who is at least one level of supervision higher, then contact BHRM to obtain authorization for testing. It is essential that the observations be communicated as soon as possible due to safety concerns and the rapid depletion of alcohol as a result of the body's metabolism.

- Observable phenomena while at work, such as direct observation of drug and/or alcohol use or the physical symptoms or manifestations of being under the influence of a drug; abnormal conduct or erratic behavior while at work or a significant deterioration in work performance;

- A report of drug or alcohol use, provided by a reliable and credible source, which has been determined to be valid by a second source;

- Evidence that an individual has tampered with a drug test during employment with the department;

- Information that an employee has caused, or contributed to, an accident while at work, where such information is consistent with possible drug use; or

- Evidence that an employee has used, possessed, sold, solicited or transferred drugs while working or while on the department's premises, or while operating the department's vehicle, machinery or equipment.

Transportation. Division management shall arrange the appropriate transportation for the employee to be transported to the drug testing facility as identified and guided by BHRM. The manager may utilize local transportation service (Taxi or Uber) to transport employee to nearest facility. This is payable with the manager's PCard.

Return-to-Duty Test. An employee in a CDL designated position who had a first time confirmed positive drug test result will have to successfully pass this type of drug test before being allowed to return to their duties.

Follow-up Test. An employee may be required to take a drug test when the employee is in an Employee Assistance Program (EAP) treatment plan due to alcohol or drug-related reasons. Such testing may or

may not be at the employee's expense. An employee in a CDL designated position will be subject to a minimum of six (6) unannounced follow-up drug tests within the first 12 months following their eligibility to return-to-duty.

Temporary Assignment. During the period after testing for suspected drug or alcohol use or when a confirmed positive drug test result has been received by the department, an employee in a safety-sensitive or CDL designated position will be assigned temporary duties within the department or placed on appropriate leave until the department has determined any action to be taken. A sworn law enforcement employee shall be placed on appropriate leave until the department has determined any action to be taken.

Overview of the Drug Testing Process.

TRAINING

Persons designated to supervise CDL drivers in designated positions shall receive at least 60 minutes of training on alcohol misuse and receive at least an additional 60 minutes of training on controlled substances use. This training is available via the online LMS in the People First System and is titled "DOT: Reasonable Suspicion (Drug and Alcohol Awareness)". The training will be used by the supervisors to determine whether reasonable suspicion exists to require a driver to undergo testing under Title 49 Part 382.603 CFR. The training includes the physical, behavioral, speech, and performance indicators of probable alcohol misuse and use of controlled substances. Recurrent training for supervisory personnel is not required.

TEST RESULTS

The drug test result of an applicant or an employee will be confidential. Due to the confidentiality requirement, the laboratories authorized to conduct drug testing will provide all positive and negative drug test results to the department's contracted Medical Review Officer (MRO). The MRO will review the test results and have the results submitted to BHRM designated contact. The BHRM contact will then notify the appropriate division director or designee.

The BHRM contact will be responsible, within five (5) working days after receiving a confirmed positive drug test result, for informing the employee in writing of a confirmed positive drug test result, the consequences of such a result, and the options available to the employee.

Upon request, the applicant or employee can obtain a copy of their drug test results from BHRM.

DISCIPLINARY ACTION AND EMPLOYEE ASSISTANCE PROGRAM (EAP)

If an applicant or employee refuses to submit to a scheduled drug test, without a reason which is acceptable to the department, the department will have cause to not hire the applicant or to discipline the employee, up to and including dismissal.

The department will refer an employee, except an employee in a sworn law enforcement position, who has a first time confirmed positive drug test result, to the EAP. The employee treatment costs for the EAP will be

paid by the employee or their health insurance program. The department and the employee will sign a confidential agreement incorporating the provisions of the EAP treatment for the employee and any department requirements. A sworn law enforcement employee will be subject to disciplinary action up to and including dismissal for the use of illegal drug or inappropriate use of alcohol. An employee in a CDL position or an employee in a safety-sensitive position shall be reassigned from their current position to a non-CDL or non-safety-sensitive position while the rehabilitation program is in effect, or placed on appropriate leave, while participating in EAP or an alcohol and drug rehabilitation program.

An employee in a sworn law enforcement position who has a confirmed positive drug test result will be placed on appropriate leave until the department has determined any action to be taken.

An employee, except those in a sworn law enforcement position, may not be disciplined or discharged on the sole basis of a first confirmed positive drug test.

Except for an employee in a sworn law enforcement position, once the employee successfully completes either the EAP or another alcohol and drug rehabilitation program, the employee will be reinstated to the same or equivalent position that he/she held prior to such rehabilitation.

CONFIDENTIALITY

All information, interviews, reports, statements, memoranda, and drug test results, written or otherwise, received or produced as a result of the drug testing program are confidential communications and are exempt from the provision of public records law, Section 112.0455 (11), F.S.

The drug testing records may not be used or received in evidence, obtained in discovery or disclosed in any public or private proceedings except:

- By order of a hearing officer or a court of competent jurisdiction pursuant to an appeal or grievance taken under this rule, or where deemed appropriate by a professional or occupational licensing board in a related disciplinary proceeding;
- To certifying bodies of sworn law enforcement or CDL designated members relative to confirmed positive drug test results; or
- To the applicant or employee who was tested and voluntarily signs a consent form.

EMPLOYEE RIGHTS

Any employee who is disciplined, or who applies for a sworn law enforcement position, a safety-sensitive position, or a CDL designated position and is not selected based on a confirmed positive drug test result, may file an appeal with the Public Employee Relations Commission (PERC) in accordance with Section 110.227, F.S. and Section 447.401, F.S.

Any appeal must be filed within 30 calendar days of receipt by the employee of notice of discipline or refusal to select. The notice will inform the employee of the right to file an appeal or, if available, the right to file a grievance under a collective bargaining contract.

Appeals to PERC will be the only administrative remedy for any employee who is disciplined or who is not selected.

An employee covered by a collective bargaining agreement may file a grievance under that contract. In no case may the employee file both an appeal and a grievance.

Any person alleging a violation of Section 112.0455, F.S., that is not appealable to PERC or an arbitrator, may file a claim in civil court to have the action set aside or to obtain damages, or both. The time limit for filing the claim is 180 days from the date the final action was taken by the department. An employee is not required to appeal or grieve before filing a civil action.

REPORTING ARRESTS

Employees shall report to their supervisor any arrest, criminal citation and/or notice to appear within three (3) business days of occurrence. Immediately upon notification the supervisor shall report to their division director, the Office of the Inspector General via Candie.Fuller@FloridaDEP.gov and BHRM, Employee Relations via HR_ER@FloridaDEP.gov. The notification will include the nature of the charge, the name of the arresting agency and a copy of the arrest warrant and/or law enforcement report. If retained as an employee subsequent to the arrest, the employee is required to keep supervisory personnel apprised of the status of the case.

Failure to report an arrest, criminal citation and/or notice to appear will be considered violation of policy regardless of the reason for arrest and/or disposition and will subject the employee to discipline and possible administrative action up to and including dismissal. The matter will be reviewed by BHRM to determine if the charge(s) conflicts with the employee's ability to perform their assigned job duties, applicable statutes, or imposes liability and risk to the Department.

RETENTION OF RECORDS.

The department shall maintain records of its alcohol misuse and controlled substances use prevention programs as provided in this section. The records shall be maintained in a secure location with controlled access. The period of retention shall comply with Title 49 Part 382.401 CFR.

DEFINITIONS:

Applicant (job applicant). A person who has applied for a (sworn law enforcement) position, safety-sensitive position, or CDL designated position with the department and has been offered employment conditioned upon successfully passing a drug test.

Commercial Driver License (CDL). A license designated one to drive a commercial motor vehicle or combination of motor vehicles used to transport passengers or property that has a gross or combined gross weights rating of 26,001 or more pounds. This includes vehicles used to transport 16 or more passengers or to transport hazardous materials requiring a placard.

Confirmation Test. A second analytical procedure used to identify the presence of a specific drug or metabolite in a specimen.

Drug. Means alcohol, including distilled spirits, wine, malt beverages, and intoxicating liquors, amphetamines; cannabinoids; cocaine; phencyclidine (PCP); hallucinogens; methaqualone; opiates; barbiturates, benzodiazepines; synthetic narcotics; designer drugs; or a metabolite of any of the substances listed herein.

Drug Testing Facility. A collection site contracted to conduct drug testing of applicants and employees of the department in accordance with applicable laws and rules.

Initial Drug Test. Means a sensitive, rapid and reliable procedure to identify negative and presumptive positive specimens.

Medical Review Officer. A licensed physician with knowledge of substance abuse disorders, laboratory testing procedures and chain-of-custody collection procedures, who possesses the appropriate medical training to interpret and evaluate an individual's positive test result together with their medical history or any other biomedical information.

Negative Drug Test. A specimen of an applicant or employee that has shown through initial or confirmation testing procedures to not contain or to be under the specified amount of drugs or metabolites.

Positive Drug Test. A specimen of an applicant or employee that has shown through initial or confirmation testing procedures to contain or to be over the specified amount of drugs or metabolites.

Prescription or Non-Prescription Medication. A drug or medication obtained pursuant to a prescription as defined by Section 893.02, F.S., or a medication that is authorized pursuant to federal or state law for general distribution and use without a prescription in the treatment of human diseases, ailments or injuries.

Reasonable Suspicion Drug Testing. A drug test based on a belief that an employee is using or has used drugs in violation of the employer's policy drawn from specific objective and articulable facts and reasonable inferences drawn from those facts in light of experience.

Safety-Sensitive Position. Any position, including a supervisory or management position, in which a drug impairment would constitute an immediate and direct threat to public health or safety.

Sworn Law Enforcement. Any employee who is required, as a condition of employment, to be certified under Chapter 943, F.S.

Administrative Directive
DEP 421

Approved by the Secretary
Effective: December 1, 2019

Violence-Free Workplace

The Department of Environmental Protection (Department/DEP) seeks to maintain an environment that avoids or minimizes workplace violence and other related issues. This policy establishes procedures that minimize the threat of violence in the workplace, without restricting appropriate public access to DEP facilities, and provides guidelines for responding promptly and effectively to workplace violence. DEP intends to adhere to the provisions of the Florida Statutes as it pertains to this policy.

Violence in the workplace poses a threat to the safety of employees and the public. Therefore, the Department has zero tolerance for violence in the workplace.

The Department has also adopted a zero tolerance for any type of violence by any individual while off duty, which could impede the Department's efforts to achieve its goals, bring discredit to the Department, or impair the operation or efficiency of the Department or of any employee.

The Department strictly prohibits, and will not tolerate, any type of verbal abuse, threats, or violence by any individual while in its offices, facilities, worksite's, vehicles or during the performance of state business. This includes violent, aggressive or threatening behavior (oral or physical) that has the potential to or does result in physical injury or otherwise places any person's safety or productivity at risk.

Such conduct includes:

- The use of force with the intent to cause harm (physical attacks, any unwanted contact such as hitting, fighting, pushing or throwing objects);
- Acts or threats that are intended to intimidate, harass, threaten, coerce, or cause fear of harm whether directly or indirectly; or
- Acts or threats made directly or indirectly by oral or written words that communicate a direct or indirect threat of physical or mental harm.

The Department will take all complaints of workplace violence seriously and will address all occurrences of threating or violent behavior. All threats will be assumed to have been made with the intent to carry them out.

All employees should take necessary steps to ensure their own safety and security. In the event of imminent life-threatening situation or perceived serious aggressive behavior, employees should attempt to retreat to a safe location and call 911. Employees are not expected to place themselves at risk by intervening in any violent event.

The Department will take immediate corrective action against perpetrators of such acts in accordance with this directive and Directive DEP 435, Conduct of Employees.

Employees must inform supervisors of any injunctions prohibiting contact between the employee and another person.

Workplace Violence Prevention

Proactive Prevention and Pre-employment Screening

The first step is to include a thorough screening of all potential job candidates through education verification, reference checking, and where required, background assessments through the Florida Department of Law Enforcement (FDLE).

- All "Positions of Trust" require a background assessment with Florida Department of Law Enforcement (FDLE) and must submit to fingerprinting.

- Training. The Department will encourage and promote workplace violence education and provide training during the New Hire Orientation process and the Annual Workplace Refresher training.

Retaliation. Retaliatory action against anyone acting in good faith who has made a complaint of workplace violence, or reported an incident of violence, or participated in an investigation concerning workplace violence is strictly forbidden. Any person found responsible for retaliatory action may be subject to corrective action up to and including dismissal.

Reporting Incidents

It is the responsibility of all Department supervisors, managers or their respective authorized designees to address occurrences of violence or perceived violence in accordance with this directive.

- In the event of any imminent life-threatening situation or perceived serious aggressive behavior, attempt a safe escape and then call 911. Employees are not expected to place themselves at risk by intervening in any violent event;
- Ensure that all appropriate managers, including the director or designee, are apprised of the situation;
- Notify the Office of the Inspector General (OIG) and the Bureau of Human Resource Management (HR) promptly of threats or perceived threats of violence;
- Ensure that all safety policies and procedures involving workplace security, including this directive are clearly communicated to employees.

Any employee involved in, or who witnesses, or otherwise becomes aware of imminent and dangerous actions such as personal injury, use or threats of weapons should first attempt a safe escape, call 911 and then inform their direct supervisor or next level manager. Employees are responsible for ensuring a manager is contacted.

Any employee involved in, or who witnesses, an incident without weapons or personal injury should still report it immediately to their respective supervisor/manager and/or HR.

Any employee who has been arrested for a third-degree misdemeanor or higher for a violent offense; has been issued an injunction; has filed an injunction or is convicted for an incident of domestic or other violence, shall report such information to his/her immediate supervisor, the OIG and HR within 24 hours receipt or the next working day. A copy of the injunction must be provided to the supervisor and the OIG immediately upon request.

Supervisors/managers have a responsibility to take all reported incidents seriously and contact the appropriate authorities.

Accommodations

Managers will make reasonable accommodations to modify the workplace or work activities to heighten security and safety for any employee subject to be a victim of aggressive or violent behavior. Such accommodations may include granting leave with or without pay, adjusting schedules or work assignments for activities such as medical and legal assistance, court appearances, counseling and relocation.

In the case of an employee, or a family or household member of the employee, who is (are) the victim(s) of domestic or sexual violence or those with reasonable cause to believe they are in imminent danger of becoming the victim of any act of domestic or sexual violence, may request additional leave. An employee seeking additional leave must exhaust all annual or personal leave, and sick leave that is available to them before being granted additional leave. Additional leave may be granted to an employee for up to three working days (if the employee has been employed for at least three months) in any 12-month period and under certain conditions:

- Seek an injunction for protection against domestic or sexual violence;
- Obtain medical care or mental health counseling or both, for the employee or a family or household member to address physical or psychological injuries resulting from the act of domestic or sexual violence;
- Obtain services from a victim-services organization;
- Make the employee's home secure or seek new housing;
- Seek legal assistance to address issues arising from the act of domestic or sexual violence and to attend and prepare for court-related proceedings arising from the act of domestic or sexual violence.

All request for leave must be approved by the employee's supervisor.

Except in cases of imminent danger to the health or safety of the employee, or to the health or safety of a family or household member, an employee seeking leave from work under this section must provide to his or her employer appropriate notice of the leave along with sufficient documentation of the act of domestic violence or sexual violence.

Employees are free to exercise their rights under this section without reprisals or retaliation and /or discrimination of any kind.

Confidentiality

Treat any employee who is a victim of violence with sensitivity and confidentiality.

Written request for leave under this section and any time sheet that reflects such request are confidential and exempt s. 119.07(1) and s.24(a), Article I of the State Constitution until 1 year after the leave has been taken.

Pursuant to s.119.071(2) 2(j) any document that reveals the identity, home or employment telephone number, home or employment address or personal assets of the victim of a crime and identifies that person

as the victim of certain crimes, including domestic and sexual violence, is confidential for a term of five years provided the victim makes a written request that such information be held confidential.

Qualified victims of domestic violence may seek entry into the *Address Confidentiality Program for Victims of Domestic Violence* as held by the Office of the Attorney General. Participants in this program are provided with an address designated by the Attorney General as a substitute mailing address to prevent their assailant(s) from finding them.

Victim Intervention and Assistance Procedures

An employee who is or may be a victim of violence and needs assistance may contact his or her supervisor, OIG, HR or the EAP directly so that appropriate measures may be taken regarding safety, security, referral to counseling and if necessary, law enforcement.

An employee who is having trouble controlling aggressive behavior or who is or may be a perpetrator of violence and needs assistance may contact his or her supervisor, OIG, HR or the EAP directly so that appropriate measures may be taken regarding obtaining assistance.

Disciplinary and Corrective Procedures

All employees are expected to adhere to safe work practices, to treat others with respect and dignity and to maintain conduct always in an aggression-free and violence-free manner. Verbal or physical threats or aggressive or violent actions in the workplace or during off-duty hours are strictly prohibited. Acts of prohibited behavior will result in serious disciplinary action, up to and including dismissal.

Violence and sexual or domestic violence convictions, including an injunction against an employee for protection relating to violent situations, may result in mandatory appropriate counseling, or if perpetrated against a Department employee may result in disciplinary action up to and including dismissal.

An employee who is convicted or who has been the subject of an OIG investigation with a sustained finding for a FIRST or subsequent occurrence of domestic or other violence will receive discipline in accordance with DEP Directive 435, up to and including dismissal.

An employee who is convicted or who has been the subject of an OIG investigation with a sustained finding by the OIG of a SECOND or subsequent occurrence of domestic or other violence shall be dismissed, unless there are compelling mitigating circumstances.

Definitions

Aggression. A physical or verbal act which implies a disposition to dominate or intrude upon others in disregard of their rights or a fight.

Assault. As defined in s. 784.011, F.S., an intentional unlawful threat by word or act to do violence to the person of another, coupled with an apparent ability to do so and doing some act which creates a well-founded fear in such other person that such violence is eminent.

Battery. As defined in Chapter 784.03 F.S., the offense of battery occurs when a person intentionally touches or strikes another person against the will of the other or intentionally causes bodily harm to another person.

Conviction. The act of being found guilty of committing a felony or third degree or greater misdemeanor by a court of law and includes a plea of *nolo contendere* or having adjudication withheld for a felony or first degree or greater misdemeanor.

Department. The Florida Department of Environmental Protection.

Domestic Violence. As defined in Chapter 741.28(2), F.S., any assault, aggravated assault, battery, aggravated battery, sexual assault, sexual battery, stalking, aggravated stalking, kidnapping, false imprisonment or any criminal offense resulting in physical injury or death of one family or household member by another family or household member or any crime designated by the court as domestic violence.

Employee Assistance Program (EAP). The Department's Employee Assistance Program (EAP) is an employee benefit program intended to help employees deal with personal problems.

Employee. A Department Career Service (CS), Selected Exempt Service (SES), Senior Management Service (SMS) and Other Personal Service (OPS)employee.

Employer. As defined in s. 440.02(16), F.S., means the state and all political subdivision thereof, all public and quasi-public corporations therein, every person carrying on any employment and the legal representative of a deceased person or the receiver or trustee of any person, employment agencies, employee leasing companies and similar agents who provide employees to other employers.

Family. As defined in s.741.28 (3), F.S., means spouse, former spouse, persons related by blood or marriage, persons who are presently residing together as if a family or who have resided together in the past as if family and persons who are parents of a child in common. The family or household members must be currently residing or have in the past resided together in the same single dwelling unit.

Harassment. An act or course of conduct directed at a specific person that, 1) causes substantial emotional distress in such person and, 2) serves no legitimate purpose. "Course of Conduct" means a series of acts over a period of time, however short, indicating a continuity of purpose.

Household Member. See Family

Injunction. Refers to a court order entered to protect an individual against violence or repeated violence. This includes injunctions received prior to the employee's employment by the Department.

Perpetrator. An employee who threatens or perpetrates an act of violence, including domestic or sexual violence.

Sexual Violence. As defined in s. 784.046 F.S., means sexual battery, a lewd or lascivious act committed on or in the presence of a person under the age of 16, luring or enticing a child, any forcible felony wherein a sexual act is committed or attempted, or any crime, the underlying factual basis of which has been found by a court to include an act of sexual violence.

Supervisor Referral. Referral of an employee to the EAP by the employee's supervisor or appropriate authority.

Victim. An individual who suffers personal physical injury or emotional trauma or death because of a threat or an act of domestic or sexual violence.

Weapon. A device, instrument or material which is used or intended to be used in the destruction of life or the infliction of bodily injury.

Administrative Directive
DEP 435

Effective October 27, 2025

Conduct of Employees

This directive establishes a system of discipline for employees of the Department of Environmental Protection (Department).

AUTHORITY

Public Officers, Employees, and Records State Employment , Section 110.227, Florida Statutes
Public officers and Employees: General Provisions, Chapter 112, Florida Statutes
Attendance and Leave, Rule 60L-34, Florida Administrative Code
Performance Evaluation System , Rule 60L-35, Florida Administrative Code
Conduct of Employees, Chapter 60L-36, Florida Administrative Code

OVERVIEW

Violations of the Department's conduct standards are unacceptable. If it is deemed necessary to discipline an employee for violation of these standards of conduct, the director or designee and Human Resource Officer or designee must review and approve all forms of discipline prior to administering disciplinary action.

Permanent career service employees may be disciplined only for "cause" as defined in this directive. Prior to taking disciplinary action, management should ensure employees are aware of what is expected of them. There shall be evidence that the employee failed to comply with acceptable conduct and performance standards. Discipline must be based on facts and documented information, not on hearsay, conjecture or unfounded conclusions.

Employees outside the permanent career service may be disciplined up to and including dismissal at will. Disciplinary actions, which generally apply to permanent Career Service (CS) employees, may also be applied to Other Personal Service (OPS), Selected Exempt Service (SES) or Senior Management Service (SMS) employees. SMS employees may only be disciplined with approval from the Department Secretary or designee.

The Department will ensure compliance with Sections 112.532, F.S. and 112.533, F.S. ,regarding law enforcement officers' rights when pursuing disciplinary actions.

MANAGEMENT'S RESPONSIBILITIES

Management is responsible for ensuring that reasonable, consistent, and uniform disciplinary actions are equitably applied, and employees are aware of management's expectations for acceptable behavior and job performance. Supervisors are responsible for providing employees with coaching and meaningful feedback regarding job performance throughout the evaluation period and recognizing violations and for recommending appropriate corrective and/or disciplinary action. Supervisor shall timely inform the employees in writing of performance expectation deficiencies that could result in a "Below Expectation" or "Unacceptable" rating and the necessary corrective action to be taken prior to the end of the evaluation period.

Supervisors should make a good faith effort to initiate counseling or disciplinary action within sixty (60) days of actual knowledge of the event giving rise to the action. The Bureau of Human Resource Management (BHRM), employee relations team must be consulted prior to initiating discipline.

STANDARDS OF CONDUCT (Types of Offenses Warranting Disciplinary Action)

Chapter 60L-36, F.A.C., sets forth the minimal standards of conduct. Employees without permanent status in the Career Service System may be dismissed at will. Permanent Career Service employees may be suspended or dismissed only for cause, which shall include, but not be limited to, the following categories. Examples under the categories listed below are not exhaustive.

1. Poor Performance. Employees shall strive to perform at the highest level of efficiency and effectiveness

    a. Employees are expected to be reliable and dependable, for example: to show up for work, ready to work on a reliable basis; to observe established work hours and scheduled appointments; to complete work on time; and to obtain permission before being off work and to schedule leave in a manner that minimizes work disruption.

    b. Employees are expected to be effective, for example: to organize their work; to stay focused on job related activities during work hours; to provide the level of effort necessary to get the job done; to demonstrate willingness and ability to make decisions and exercise sound judgment; to produce work that consistently meets or exceeds expectations; to accept responsibility for their actions and decisions; to adapt to changes in work assignments, procedures, and technology; and to be committed to improving individual performance.

2. Negligence. Employees shall exercise due care and reasonable diligence on the performance of job duties.

3. Inefficiency or Inability to Perform Assigned Duties. Employees shall, at a minimum, be able to perform duties in a competent and adequate manner.

4. Insubordination. Employees shall follow lawful orders and carry out the directives of persons with duly delegated authority. Employees shall resolve any differences with management in a constructive manner.

5. Violation of Law or Department Rules. Employees shall abide by the law and applicable rules and policies and procedures, including those of the employing agency and the rules of the State Personnel System. All employees are subject to Part III of Chapter 112, F.S., governing standards of conduct, which agencies shall make available to employees. An agency may determine that an employee has violated the law even if the violation has not resulted in arrest or conviction. Employees shall abide by both the criminal law, for example, drug laws, and the civil law, for example, laws prohibiting sexual harassment and employment discrimination.

6. Conduct Unbecoming a Public Employee. Employees shall conduct themselves, on and off the job, in a manner that will not bring discredit or embarrassment to the state.

    a. Employees shall be courteous, considerate, respectful, and prompt in dealing with and serving the public and co-workers.

b. Employees shall maintain high standards of honesty, integrity, and impartiality. Employees shall place the interests of the public ahead of personal interests. Employees shall not use, or attempt to use, their official position for personal gain or confidential information for personal advantage.

c. Employees shall protect state property from loss or abuse, and shall use state property, equipment and personnel only in a manner beneficial to the Department.

7. Misconduct. Employees shall refrain from conduct which, though not illegal or inappropriate for a state employee generally, is inappropriate for a person in the employee's particular position. For example, cowardice may be dishonorable in people generally, but it may be entirely unacceptable in law enforcement officers. By way of further example, people are generally free to relate with others, but it may be entirely unacceptable for certain employees to enter into certain relations with others, such as correctional officers with inmates.

8. Habitual Drug Use. Agencies shall not tolerate violations of Florida's Drug Free Workplace Act, .or other misuse of mood or mind-altering substances, including alcohol and prescription medications.

9. Conviction of Any Crime. Including a plea of nolo contendere and a plea of guilty with adjudication withheld.

INQUIRIES AND INVESTIGATIONS

An informal inquiry may be conducted to question an employee about an alleged act of misconduct. Prior to conducting any informal inquiry, management shall consult with the Office of Inspector General, Office of General Counsel and/or BHRM for guidance.

Formal allegations of misconduct will be investigated by the Office of Inspector General, as provided in DEP 290, Internal Investigations Directive. Investigations of law enforcement officers will be conducted in accordance with the Officers' Bill of Rights.

An employee may request representation at an inquiry or investigative interview and such request must be granted. However, the employee must be made aware that any costs associated with representation are at the employee's expense and will not be borne by the state.

If an employee is under investigation for a violation for which dismissal may be a penalty, the Human Resource Officer may authorize that the employee be placed on administrative leave in accordance with Rule 60L-34.0071(3)(f), Florida Administrative Code. An employee placed on administrative leave shall be provided with written notice prepared by the BHRM advising them of the purpose, terms, and conditions of the administrative leave. A copy of such notice will be placed in the employee's personnel file.

REPORTING ARRESTS

Employees shall report to their supervisor any arrest, criminal citation and/or notice to appear within three (3) business days of occurrence. Immediately upon notification the supervisor shall report to their division director the Office of the Inspector General via Candie.Fuller@FloridaDEP.gov and BHRM, Employee Relations via HR_ER@FloridaDEP.gov. The notification will include the nature of the charge, the name of the

arresting agency and a copy of the arrest warrant and/or law enforcement report. If retained as an employee subsequent to the arrest, the employee is required to keep supervisory personnel apprised of the status of the case.

Failure to report an arrest, criminal citation and/or notice to appear will be considered violation of policy regardless of the reason for arrest and/or disposition and will subject the employee to discipline and possible administrative action up to and including dismissal. The matter will be reviewed by BHRM to determine if the charge(s) conflicts with the employee's ability to perform their assigned job duties, applicable statutes, or imposes liability and risk to the Department.

CORRECTIVE ACTIONS

It is the supervisor's responsibility to counsel employees regarding expected conduct and performance. Counseling may occur informally or formally. Counseling documents are not considered discipline and are not placed in the employee's personnel file. Employees shall be timely informed in writing of performance expectation deficiencies that could result in a "Below Expectation" or "Unacceptable" rating and the necessary corrective action to be taken prior to the end of the evaluation period.

Informal Counseling. A discussion by management with an employee noting area(s) needing improvement.

Formal Counseling. Counseling that is documented in writing by management to the employee on a Letter of Concern, DEP 54-100, outlining areas of concern about an employee's performance and/or behavior and what corrective action is needed for the employee to achieve an acceptable level. A copy of an issued Letter of Concern shall be provided to HR_ER@FloridaDEP.gov.

DISCIPLINARY ACTIONS

Disciplinary action types include but are not limited to the following:

1. Reprimand.

   The Official Reprimand, DEP-54-104, should indicate the nature of the problem, cite the standard of conduct violated, the date or timeframe, provide a brief description of the misconduct and circumstances warranting the reprimand.

   a. Supervisors shall propose action and submit through their chain-of-command as required. After the action has been approved within the division/office, a draft will be submitted to BHRM, Employee Relations HR_ER@FloridaDEP.gov for review and approval.

   b. Management will give the original Reprimand to the employee to sign acknowledging receipt. A copy is sent to the BHRM for inclusion in the employee's personnel file.

   c. The employee cannot appeal the Reprimand to the Public Employee Relations Commission, but it can be grieved through the union's grievance procedure or the Department's internal grievance procedure, ADM 440, Career Service Employee Grievances Policy.

2. Reduction in Pay, Disciplinary Demotion, Involuntary Transfer (more than 50 miles by highway).

3. Suspension and Dismissal for Employees with Permanent Status in the Career Service System.

Management is responsible for recommending such actions for serious violations of conduct standards or performance expectations by employees. Supervisors shall propose action and submit through their chain-of-command for approval by the division director or delegate. After the action has been approved, the division director will submit to BHRM, Employee Relations HR_ER@FloridaDEP.gov for review and approval.

If approved, BHRM will prepare a letter of action to the employee. The letter will be either hand delivered to the employee or mailed via certified mail, return receipt requested.

Per Section 110.217(3), F.S., if an employee who has received an internal agency promotion from a position in which the employee held permanent status is to be dismissed from the promotional position for failure to meet the established performance standards of the promotional position while in probationary status, the agency, before dismissal, shall return the employee to his or her former position, or to a position with substantially similar duties and responsibilities as the former position, if such a position is vacant. Such determinations by an agency are not appealable, and this subsection does not apply to dismissals for any other reason.

Before taking any of these types of actions listed in #2 or #3 against an employee with permanent status in the Career Service System, a "Notice of Intent" letter must be given to the employee prior to administering the discipline. BHRM will prepare the document. The employee shall receive written notice of such action at least 10 calendar days prior to the date of the proposed final action. The "Notice of Intent" letter will contain the following elements:

a. A statement that no action will be taken until a "Final Notice" letter is received by the employee.

b. The basis for the suspension, demotion, reduction in pay, involuntary transfer or dismissal, including which standard(s) of conduct that the employee is alleged to have violated.

c. The dates and circumstances surrounding the alleged violation(s).

d. A description of the supporting elements or documentation establishing that "cause" exists to take the action. This may be documentary evidence, witness identification, statements, or other evidence. This is an important "cause" element of notice to the employee to provide the employee with the same information in the possession of the Department and thereby give the employee sufficient information in order to refute or rebut the allegations.

e. Notice of the right to request a predetermination conference within five business days of receipt of the "Notice of Intent" in accordance with Section 110.227(5)(a), Florida Statutes. BHRM is responsible for setting up the predetermination conference and ensuring the director is prepared to preside over the meeting. The predetermination conference affords the employee an opportunity to appear before the agency or official taking the action to answer orally and in writing the charges against them.

f. The "Notice of Intent" letter may be electronically delivered, hand delivered, sent by certified mail or by other delivery services. A signed copy of the "Notice of Intent" letter shall be sent to BHRM.

g. Predetermination Conference.

(1) If the employee requests a predetermination conference, the person who has final decision-making authority (e.g., director) or their designee must conduct the predetermination conference.

(2) The predetermination conference attendees will ordinarily be limited to the following: employee, their representative, the director or designee, the employee's manager, Human Resource Officer and/or Employee Relations Manager and the General Counsel or designee.

(3) The purpose of the predetermination conference is to enable the employee to refute or rebut the allegations contained in the "Notice of Intent" letter, provide their explanation for the alleged misconduct, and provide reasons why the proposed action is too severe if the allegations are true.

(4) The conference shall not be used as a forum to argue the merits of the proposed action or to interrogate the employee. Questions may be asked by any of the conference attendees to clarify the employee's statements.

(5) The BHRM will electronically record the conference to preserve an accurate and complete record of the proceedings. The employee shall be notified at the outset of the conference that a copy of the recording will be furnished to them upon request. The original recording will be maintained by BHRM as the official custodian of employee files.

(6) If the employee chooses to not have a conference, the director or designee will make a final decision with approval of the Human Resource Officer or designee and the General Counsel or designee.

h. Final Decision and Notice.

(1) The director or designee will make a final decision, following the conference, with the approval of the Human Resource Officer or designee and the General Counsel or designee. If the decision is made to proceed with the disciplinary action or alternatively to take no further action or reduce the level of discipline proposed, BHRM will prepare a "Final Notice" letter to the employee advising the employee of the decision. If disciplinary action is taken, this final notice will inform the employee of their right to either grieve under the collective bargaining agreement (if applicable) or appeal to the Public Employee Relations Commission within 21 days of receipt of the "Final Notice" letter.

(2) The Department's action will proceed even if the employee appeals.

4. Suspensions, Reductions in Pay, Demotions and Dismissal of Employees **without** Permanent Career Service System Status (Other Personal Services, Probationary Career Service, Select Exempt Service or Senior Management Service).

A career service employee with performance deficiencies who has been promoted with probationary status may be demoted to their former position or a comparable position if one is vacant. If such a

position is not available before dismissal, the Department shall make a reasonable effort to retain the employee in another vacant position. Otherwise, the supervisor may recommend probationary dismissal to their division director.

a. The procedure for taking appropriate disciplinary action against an employee without permanent status in the Career Service System differs in that the employee is not entitled to a predetermination conference or the right to grieve or appeal the action to the Public Employee Relations Commission.

b. The BHRMwill prepare the letter for the appropriate disciplinary action for the director or designee's signature and distribution to the employee advising the employee of the action to be taken and the effective date.

c. After transmittal to the employee, a signed copy of the notice will be sent to the BHRMfor placement in the employee's personnel file.

d. Although employees lacking permanent status in the Career Service System do not have the right to appeal to the Public Employee Relations Commission or grieve under any collective bargaining agreement, all employees are protected under federal and state laws barring unlawful discrimination in employment.

5. Extraordinary Situations.

Extraordinary situations may exist when the retention of a career service employee with permanent status would result in damage to state property, be detrimental to the best interest of the state or would result in injury to the employee, a fellow employee, or some other person. In these situations, employees may be suspended or dismissed without ten (10) days prior notice, provided that written or oral notice of such action, evidence of the reasons therefore, and an opportunity to rebut the charges are furnished to the employee prior to such suspension or dismissal. Such notice may be delivered to the employee personally or may be sent by certified mail with return receipt requested.

In certain situations, in consultation with BHRM, the director or designee may temporarily assign other duties to the employee, temporarily relocate the employee, or the Human Resource Officer may place the employee on administrative leave in accordance with Rule 60L-34.0071(3)(F), Florida Administrative Code.

In all cases, the director or designee is expected to discuss the circumstances warranting the action with the Human Resource Officer or designee before taking any action under the extraordinary procedure's provisions.

(1) Any employee who is suspended or dismissed pursuant to the provisions of this paragraph may grieve under the collective bargaining agreement (if applicable) or appeal to the Public Employees Relations Commission within 21 days of receipt of the dismissal letter.

DEFINITIONS

Administrative Leave. For purposes of this directive, a type of paid leave a Career Service, Select Exempt Service or Senior Management Service employee may be required to take because of a formal Department investigation for violation of a rule or statute.

Cause. Adequate or sufficient reason or grounds to take an action. Cause shall include, but is not limited to, violations of the Standards of Conduct set forth in Chapter 60L-36, F.A.C.

Demotion. A change in the classification of an employee to a broadband level having a lower maximum salary or that changes the classification of an employee to a broadband level having the same or a higher maximum salary, but a lower level of responsibility.

Informal Inquiry. An informal gathering process to verify circumstances or allegations of a minor nature that would likely result in disciplinary action. An informal inquiry may also be undertaken to determine whether an investigation may be warranted.

Letter of Concern. A non-disciplinary advisory letter provided to the employee by management, outlining areas of concern about the employee's behavior and/or performance and what action is needed for the employee to correct the behavior and/or performance to an acceptable level.

"Notice of Intent" Letter. This written notice letter is provided to an employee with permanent status prior to suspension, reduction in pay, demotion, involuntary transfer or dismissal. This letter, with supporting documents, is prepared by the BHRM in consultation with the Office of General Counsel.

Reduction in Pay. A disciplinary action taken in conjunction with a demotion for violation of the standards of conduct or for cause.

Reprimand. A written notice to the employee that is disciplinary in nature.

Administrative Directive
DEP 436

Approved by the Secretary
Effective January 4, 2024

Discrimination, Harassment and Sexual Harassment

This directive establishes policy relating to the review process and procedures for resolving claims of alleged discrimination and harassment, including sexual harassment, for the Department of Environmental Protection (Department or DEP).

AUTHORITY

State Employment, Chapter 110, Florida Statutes
Public Officers and Employees: General Provisions, Chapter 112, Florida Statutes
Discrimination in the Treatment of Persons; Minority Representation, Chapter 760, Florida Statutes
Equal Employment Opportunity and Affirmative Action, Rule 60L-40, Florida Administrative Code
Title VII of the Civil Rights Act of 1964

OVERVIEW

The Department maintains that every employee has a right to a workplace free of discrimination, and harassment, including sexual harassment. Title VII of the Civil Rights Act prohibits discrimination and harassment by any person who is present in the workplace, even if not employed by the Department.

EMPLOYEE'S RESPONSIBILITIES

The Department has zero tolerance for all forms of harassment and discrimination. Employees should refrain from any behavior that is or has the potential to be perceived as discrimination or harassment. As part of the onboarding process for new hires, all employees receive training on this topic and are required to take a refresher course annually. Employees are also made aware of the definition of discrimination and harassment, including sexual harassment as contained in this directive, and in DEP 435, Conduct of Employees Directive and Rule 60L-40.001, Florida Administrative Code.

Each employee shall be given a reasonable opportunity to discuss this policy and the issues of discrimination, and harassment including sexual harassment with management (his/her immediate supervisor, Bureau Chief, Assistant Division Director, Division/Office Director), Department's Human Resource Officer, the Office of General Counsel and/or the Office of Inspector General. It is the employee's responsibility to seek clarification or ask questions to ensure a clear understanding of the directive.

MANAGEMENT'S RESPONSIBILITIES

Management is expected to create and maintain a work environment free of unwanted conduct of a sexual nature which could result in an offensive, intimidating and/or hostile workplace as well as any form of discrimination or harassment. Managers shall ensure equality of opportunity for all employees, and report complaints of discrimination and harassment, including sexual harassment to the offices designated below.

COMPLAINT FILING

Any employee, person or entity regulated by or doing business with the Department claiming to be aggrieved by discrimination and harassment, including sexual harassment as defined in this directive should immediately report the matter.

Allegations of discrimination and harassment, including sexual harassment must be made by employees or Management to the Department's Human Resource Officer, or the General Counsel or the Inspector General whom the Department has designated to receive complaints. All personal identifying information will remain confidential in accordance with the laws of the state.

Employees are not required to report the matter to their immediate supervisor.

Allegations of discrimination and harassment, including sexual harassment may be initially reported in a variety of ways, including in-person, via telephone, through postal or electronic mail, or by following the instructions as found on form DEP 54-102, Discrimination and Harassment Complaint Form. All complaints will be reduced to writing and signed by the complainant.

The filing of a complaint pursuant to this procedure shall not preclude the complainant from also filing a complaint with the Florida Commission on Human Relations (FCHR) or the Federal Equal Employment Opportunity Commission (EEOC).

If a complaint is filed with either the FCHR or the EEOC, and DEP undertakes an investigation to provide information to the FCHR or EEOC, DEP is not required to conduct an investigation otherwise required in these procedures, however, DEP shall discipline an employee who has committed sexual harassment regardless of the manner of investigation conducted.

If an employee is in a position covered by a collective bargaining agreement, which provides for an alternative procedure for making a complaint covered by this directive, the employee may use the alternative procedure in lieu of, but not in addition to, the procedure provided by this directive.

If the procedure in this directive conflicts with the collective bargaining agreement, the collective bargaining agreement should be followed.

INVESTIGATION OF COMPLAINT

All allegations of misconduct will be investigated by the Office of Inspector General as provided in DEP 290, Internal Investigations Directive. Complaints will be assigned to the appropriate Office of Inspector General staff member for investigation. The investigator assigned will investigate all specific allegations, interview any witnesses, including co-workers, supervisors and the Complainant and Respondent.

According to Executive Order No.19-11 the Department should take steps to eliminate further contact between the complainant and the subject of the complaint until the conclusion of the investigation.

Upon completion of an internal investigation with a sustained finding, the final investigative report will be distributed by the Office of Inspector General to the Director or Management authority of the subject employee(s) and the Bureau of Human Resource Management (BHRM) for review and appropriate response.

After discussion and approval by the Department's Human Resource Officer, a written decision, either dismissing the complaint or taking appropriate corrective or disciplinary action, will be rendered by management. The Complainant and Respondent will receive a written copy of the final investigative report.

Post-Investigation

Upon completion of the investigation a representative from BHRM will follow-up with the complainant and address any steps that have been taken by the Department. Additionally, other available resources such as the Employee Assistance Program will be discussed with the complainant. All personal identifying information will remain confidential in accordance with the laws of the state.

Disciplinary Action

Any employee of the Department who has discriminated, harassed or retaliated against another employee is in violation of this directive shall be subject to disciplinary action up to and including dismissal.

Any supervisory or managerial employee who has knowledge of discrimination or harassment and fails to immediately report the matter to the persons the Department has designated to receive the complaints, shall be subject to disciplinary action up to and including dismissal.

Any employee who knowingly files a false complaint of discrimination or harassment against another employee shall be subject to disciplinary action up to and including dismissal. Disciplinary actions will be administered in accordance with applicable Florida Statutes, personnel rules and Department regulations.

DEFINITIONS

Complainant. The individual(s) who has (have) filed a discrimination or harassment complaint.

Course of Conduct. A series of acts over a period of time, however short, indicating a continuity of purpose.

Discrimination. The action of making an adverse employment decision or an action that has the effect of disparate treatment for any protected classes, based on race, color, religion, sex, pregnancy, national origin, age, handicap, or marital status.

Employee. An individual employed by the Department in the Senior Management Service, Selected Exempt Service, Career Service or Other Personal Services category.

Harassment. An act or course of conduct directed at a specific person that, 1) causes substantial emotional distress in such person and, 2) serves no legitimate purpose.

Management. An individual with authority to undertake or recommend employment decisions affecting the employee even if the individual does not have the final say; or the individual has authority to direct the employee's daily work activities even if that individual does not have the authority to undertake or recommend tangible job decisions (i.e., decisions that significantly change another employee's employment status such as hiring, firing, promoting, demoting and reassigning the employee.)

Respondent. The individual(s) who is(are) the subject of a discrimination or harassment complaint.

Retaliation. Any adverse job action, threat, intimidation or coercion that is likely to deter a reasonable person from making a complaint, cooperating in the review/investigation of a complaint, participating in

any proceeding arising from a complaint or otherwise informing the Department that someone is engaging in discrimination or harassment, including sexual harassment.

Sexual Harassment. Is defined as unwelcome conduct of a sexual nature and may include: sexual advances, request for sexual favors, or other verbal or physical conduct of a sexual nature directed toward an employee or applicant. This conduct becomes unlawful when:

- Submission to such conduct is either explicitly or implicitly a term or condition of an individual's employment;
- Submission to or rejection of such conduct by an individual is used as the basis for an employment decision affecting such individual; or
- Such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile or offensive working environment.

Any questions about this directive should be directed to the Bureau of Human Resource Management.