# S.C. Public Employee Benefit Authority

## Anti-Harassment Policy

Office of Responsibility: Human Resources
Revised: March 2013

**THE LANGUAGE USED IN THIS DOCUMENT DOES NOT CREATE AN EMPLOYMENT CONTRACT BETWEEN THE EMPLOYEE AND THE AGENCY, THIS DOCUMENT DOES NOT CREATE ANY CONTRACTUAL RIGHTS OR ENTITLEMENTS. THE AGENCY RESERVES THE RIGHT TO REVISE THE CONTENT OF THIS DOCUMENT, IN WHOLE OR IN PART. NO PROMISES OR ASSURANCES, WHETHER WRITTEN OR ORAL, WHICH ARE CONTRARY TO OR INCONSISTENT WITH THE TERMS OF THIS PARAGRAPH CREATE ANY CONTRACT OF EMPLOYMENT.**

### I. Policy

It is the Public Employee Benefit Authority's policy to provide a work environment free of harassment based on race, color, religion, sex (including pregnancy), national origin, age, disability, genetic information or any other protected category under federal, state or local law.

### II. Definition

Harassment is unwelcome conduct that is based on a protected category and may become unlawful when:

enduring the offensive conduct becomes a condition of continued employment; or
it results in an adverse employment decision; or

the conduct is severe or pervasive enough to create a work environment that a reasonable person would consider intimidating, hostile, abusive or offensive.

Offensive conduct may include, but is not limited to, offensive jokes, slurs, epithets or name calling, physical assaults or threats, intimidation, ridicule, insults, offensive objects or pictures, or interference with work performance. It may also include unwelcomed sexual advances, innuendoes, requests for sexual favors, physical contact, unwelcomed and repeated propositions, or unwelcomed and repeated flirtation.

Offensive conduct may be communicated verbally, in writing, or electronically. The conduct may be between co-workers, employee to supervisor, supervisor to employee, employees/supervisors in other areas, employee to non-employee, or non-employee to employee.

## III. Prevention

Prevention is the best tool to eliminate harassment in the workplace. Employees who feel they have been subjected to offensive behavior should take the initiative in stopping the contact. Inform the harasser directly that the conduct is unwelcome and must stop. Should the harassment continue, employees are encouraged to report it to their supervisor, another member of management, or Human Resources.

## IV. Complaint Process

Employees needing to make a complaint should do so in writing to the Human Resources Director. Supervisors having knowledge of complaints or allegations of harassment are required to contact the Human Resources Director immediately. Complaints will be investigated promptly and thoroughly and as discreetly as possible. In cases where it is determined that harassment did occur, disciplinary action up to and including dismissal may be issued.

Any employee who knowingly makes false accusations or false statements during an investigation may be subject to disciplinary action up to and including dismissal.

Retaliation against individuals who file complaints or participate in complaint investigations is prohibited. Retaliation offenses should be reported to the Human Resources Director immediately.

# S.C. Public Employee Benefit Authority

## Business Casual Dress Policy

Office of Responsibility: Human Resources
Revised: March 2015

**THE LANGUAGE USED IN THIS DOCUMENT DOES NOT CREATE AN EMPLOYMENT CONTRACT BETWEEN THE EMPLOYEE AND THE AGENCY, THIS DOCUMENT DOES NOT CREATE ANY CONTRACTUAL RIGHTS OR ENTITLEMENTS. THE AGENCY RESERVES THE RIGHT TO REVISE THE CONTENT OF THIS DOCUMENT, IN WHOLE OR IN PART. NO PROMISES OR ASSURANCES, WHETHER WRITTEN OR ORAL, WHICH ARE CONTRARY TO OR INCONSISTENT WITH THE TERMS OF THIS PARAGRAPH CREATE ANY CONTRACT OF EMPLOYMENT.**

### I. Policy

The SC Public Employee Benefit Authority establishes business casual attire as acceptable dress during the work week. Employees are responsible for ensuring that their attire projects a positive image to all customers, both internal and external, at all times. This policy does not require employees to wear business casual attire. Employees who prefer to dress in traditional business attire should feel free to do so.

### II. Guidelines

Employees should use good judgment in determining what attire is appropriate. Attire at all times should be neat, clean, pressed and reflect personal pride and respect for the job. Business casual attire is intended to allow employees to feel comfortable at work yet appropriate for an office environment.

### A. Acceptable Attire

For women, business casual attire includes, but is not limited to: dresses, slacks, khaki or chino pants, skirts, sport shirts and blouses, and sweaters. Dresses and tops with less than a two inch strap across the shoulder must be covered with a jacket, shirt, or sweater. Ankle pants should fall below the calf, should be tailored, and reflect a professional look. Appropriate shoes include heels, flats, boots, and sandals. Jeans and tennis shoes can be worn on Fridays provided they are clean and without tears or holes.

For men, business casual attire includes, but is not limited to: slacks, khaki pants, dress shirts, collared shirts, sweaters, and appropriate shoes. Jeans and tennis shoes can be worn on Fridays provided they are clean and without tears or holes.

### B. Unacceptable Attire

Unacceptable attire includes, but is not limited to: wind suits, sweatpants, sweatshirts, workout attire, hospital scrubs, shorts, Bermuda shorts, T-shirts, tank tops or muscle shirts, beach attire, midriff tops, dresses or skirts that are excessively short, spandex pants, flat-heeled flip flops of any kind, rubber shoes or any recreational shoe, and house slippers. Garments which are tight and/or ill-fitting are inappropriate, as are mini-skirts, skirts with high slits, or visible undergarments.

### C. Exceptions

Employees hosting or attending meetings with customers, vendors, Board members, employees from another office/agency or applicants should consider traditional business attire. Managers and supervisors can specify business attire based on the business needs of their department. Employees needing to wear tennis shoes Monday through Thursday due to medical necessity, must provide a physician's statement to Human Resources.

## III. Responsibility

Supervisors are responsible for interpreting and enforcing this policy. Should a supervisor determine that an employee's dress is inappropriate, the supervisor will require the employee to leave the worksite and return with more appropriate dress. If an employee must leave work to change clothes, the employee must take annual leave. Repeated infractions could result in disciplinary action.

# S.C. Public Employee Benefit Authority

## Domestic Violence Policy

Office of Responsibility: Human Resources
Revised: June 2016

**THE LANGUAGE USED IN THIS DOCUMENT DOES NOT CREATE AN EMPLOYMENT CONTRACT BETWEEN THE EMPLOYEE AND THE AGENCY, THIS DOCUMENT DOES NOT CREATE ANY CONTRACTUAL RIGHTS OR ENTITLEMENTS. THE AGENCY RESERVES THE RIGHT TO REVISE THE CONTENT OF THIS DOCUMENT, IN WHOLE OR IN PART. NO PROMISES OR ASSURANCES, WHETHER WRITTEN OR ORAL, WHICH ARE CONTRARY TO OR INCONSISTENT WITH THE TERMS OF THIS PARAGRAPH CREATE ANY CONTRACT OF EMPLOYMENT.**

### I. Policy Statement

In compliance with Section 1-1-1410 of the S.C. Code of Laws, the State of South Carolina and PEBA are committed to the health and safety of employees and will not tolerate any act of domestic violence in the workplace. Should an employee's supervisor or Human Resources become aware that such an event has occurred in the workplace, off-site but on-duty, and/or through the use of State resources, the agency shall report the incident to appropriate law enforcement.

### II. Guidelines

**Any employee in immediate danger should contact 911 immediately.**

Employees are encouraged to report to law enforcement domestic violence which occurs outside of the workplace.

While perpetrators of domestic violence are encouraged to seek help, an employee who is a perpetrator of domestic violence in the workplace, off-site but on-duty, and/or using State resources, may be subject to discipline up to, and including, termination. An employee who is an alleged perpetrator and the subject of an Order of Protection or Restraining Order which affects workplace operations or the employee's ability to perform job duties, must report the order to Human Resources no later than the employee's next scheduled work day. Failure to report may result in disciplinary action up to, and including, termination.

## III. Support

An employee who experiences domestic violence is encouraged to seek assistance and to report the situation to their supervisor or Human Resources. The agency will maintain any information received outside of the employee's personnel record, and reporting will not be considered in employment decisions. The information shall be maintained confidentially and disclosure shall be limited to legitimate legal and business purposes. Under no circumstances shall the agency take retaliatory action against an employee based upon their report of experiencing domestic violence.

The SC Coalition Against Domestic Violence and Sexual Assault (SCCADVASA) website provides a list of useful resources to assist employees. Affected employees are encouraged to access resources at http://www.sccadvasa.org/sc-says-no-more/

Employees who experience domestic violence may require support from the agency. If a request for assistance is received by a supervisor or Human Resources, the agency will make every effort to provide flexibility in work schedules, security measures such as escorts to and from parking areas, and appropriate leave.

A variety of leave options may be available to employees. The agency will exercise flexibility in application of leave programs to the extent that business is not unduly disrupted. Human Resources may request appropriate documentation related to the leave. Leave options may include:

1. Sick leave for the purpose of the employee or certain family members receiving medical treatment or counseling services related to domestic violence;
2. A sick leave advance if necessary and appropriate;
3. Coverage under the Family Medical Leave Act (FMLA) if the domestic violence results in a serious health condition for the employee or certain members of the employee's family;
4. Consideration of a request for use of more than 30 days of annual leave in a year for emergency or extreme hardship conditions;
5. Consideration of the transferring of annual or sick leave to the employee from the agency's leave pool for emergency or catastrophic situations;
6. Court leave when the employee is absent for purposes of seeking an order of protection or restraining order, or assisting with the prosecution of a domestic violence case in which they are a witness or survivor; (Note: This option is not fully operative unless and until State HR Regulation 19-712.01 F is amended to allow the use of "court leave" for such purposes.); and
7. Unpaid leave may be granted if no other option is available.

Employee assistance may also be provided through Job Retention Services with the SC Vocational Rehabilitation Department. They may be reached by phone at 803-782-4239.

# S.C. Public Employee Benefit Authority

## Drug-Free Workplace and Substance Abuse Policy

Office of Responsibility: Human Resources
Revised: March 2013

**THE LANGUAGE USED IN THIS DOCUMENT DOES NOT CREATE AN EMPLOYMENT CONTRACT BETWEEN THE EMPLOYEE AND THE AGENCY, THIS DOCUMENT DOES NOT CREATE ANY CONTRACTUAL RIGHTS OR ENTITLEMENTS. THE AGENCY RESERVES THE RIGHT TO REVISE THE CONTENT OF THIS DOCUMENT, IN WHOLE OR IN PART. NO PROMISES OR ASSURANCES, WHETHER WRITTEN OR ORAL, WHICH ARE CONTRARY TO OR INCONSISTENT WITH THE TERMS OF THIS PARAGRAPH CREATE ANY CONTRACT OF EMPLOYMENT.**

### I. Purpose

The S.C. Public Employee Benefit Authority is committed to protecting the safety, health and wellbeing of all employees. The Agency is committed to maintaining a safe and secure work environment that is alcohol and drug-free.

### II. Covered Workers

Any individual that conducts business for the Agency, is applying for a position or conducting business on Agency property is covered by our drug-free workplace policy. Our policy includes, but is not limited to full-time employees, part-time employees, volunteers, interns and applicants. This drug-free workplace policy is intended to apply whenever anyone is representing or conducting business for the Agency. This policy applies during all working hours, whenever conducting business or representing the Agency, while on Agency property and at Agency-sponsored events.

### III. Prohibited Behavior

The Agency prohibits the manufacture, distribution, dispensation, sale, possession or use of illegal drugs, narcotics or controlled substances (unless use is prescribed by a licenses medical provider).

Employees shall notify their supervisor when required to use prescription medication which they have been informed has the potential to impair job performance. The employee shall advise the supervisor of the know side effects of such medication and the prescribed period of use. Employees are under no obligation to disclose prescription medication whose effects or side effects do not impair job performance.

Employees are prohibited from conducting Agency business under the influence of alcohol. Under the influence means having any detectable concentration of alcohol in the body. The use of alcohol on Agency premises or while conducting Agency business is prohibited, except at approved Agency sponsored social events. Alcohol consumption at an Agency sponsored event is completely voluntary and should be in moderation.

## IV. Guidelines

Any employee who is convicted of a criminal drug violation occurring on or off Agency premises must notify the Agency within five calendar days of the conviction. Law enforcement agencies will be notified whenever illegal drugs are found in the workplace (or contained within State property).

Employees involved in a motor vehicle accident while driving a State-owned vehicle, may be required to submit for drug and/or alcohol testing.

Violations of this policy may result in disciplinary action up to and including termination. Each case will be reviewed and necessary action will be taken. The Agency reserves the right to test employees it reasonably suspects to be using drugs or alcohol in violation of this policy.

## V. Job Retention Services

Employees in need of assistance in relation to drug or alcohol use are encouraged to contact Job Retention Services with the S.C. Vocational Rehabilitation Department, 1410 Boston Avenue, West Columbia, SC 29171 or 896.6500.

# S.C. Public Employee Benefit Authority

## ID Badge Security Policy

Office of Responsibility: Human Resources
Revised: June 2017

**THE LANGUAGE USED IN THIS DOCUMENT DOES NOT CREATE AN EMPLOYMENT CONTRACT BETWEEN THE EMPLOYEE AND THE AGENCY, THIS DOCUMENT DOES NOT CREATE ANY CONTRACTUAL RIGHTS OR ENTITLEMENTS. THE AGENCY RESERVES THE RIGHT TO REVISE THE CONTENT OF THIS DOCUMENT, IN WHOLE OR IN PART. NO PROMISES OR ASSURANCES, WHETHER WRITTEN OR ORAL, WHICH ARE CONTRARY TO OR INCONSISTENT WITH THE TERMS OF THIS PARAGRAPH CREATE ANY CONTRACT OF EMPLOYMENT.**

### I. Purpose

The purpose of this policy is to provide an additional means of establishing a safe work place for employees and a safe environment in which the public may conduct business.

### II. Scope

This policy applies to all full-time, temporary and contract employees.

### III. Policy Statement

It is the policy of the South Carolina Public Employee Benefit Authority (PEBA) that employees have the safest possible environment in which to provide the highest quality public service and that the public has a safe environment in which to conduct business. To that end, PEBA asks that all individuals working or conducting business on PEBA premises to be aware of and adhere to the following standards.

### IV. Doors and Elevators

All doors on the first floor other than those leading directly into the public Customer Intake area of PEBA are to remain closed and locked at all times. Access is restricted to employees with ID badges and escorted visitors.

Doors leading into the stairwells on the first floor are to remain closed and locked at all times. Access is restricted to employees with ID badges and escorted visitors.

Elevator access on the first floor is restricted to employees with ID badges and escorted visitors.

## V. Employees

PEBA will provide ID badges to employees that will include the name of the agency, photo of the employee and the employee's name.

Employees are asked to surrender their ID badge to their supervisor upon termination of employment or when requested.

Employees are asked to immediately report a lost ID badge to Human Resources so that the badge may be deactivated.

Employees are asked to immediately report a misplaced ID badge to Human Resources. A temporary ID badge will be activated and issued for the use of one day. At the end of the day, the employee will return the temporary ID badge to Human Resources and it will be deactivated.

An employee, who observes an individual, who is not an employee, without an ID badge in a non-public area of the premises, is asked to immediately report the individual to a supervisor or to Human Resources.

## VI. Visitors

Individuals who are not employees of PEBA but are engaged in work activities at PEBA's facility are required to sign in at the receptionist desk.

Visitors to PEBA must be escorted by an employee when on PEBA premises. Visitor badges will be provided and will be issued at the receptionist desk. Before visitors leave PEBA premises, visitor badges are to be returned to the receptionist.

Visitors going to the canteen should be escorted by an employee.

Visitors needing access beyond the first floor will be met at the elevator and escorted by an employee from the area to which they need access.

Employees are asked to not allow visitors to enter the building at any time other than the PEBA's core business hours of 8:30 a.m. to 5:00 p.m.

Employees may use the back entrance to the building to avoid after-hours contact with visitors.

## VII. Mail Room

UPS, Federal Express, DHL, US Postal Services, Interagency mail courier and the contracted mailing service will have access to make deliveries and pick-ups to the mail room through an intercom system linked directly to the mail room.

The mail room will be staffed at all times for deliveries and pick-ups.

## VIII. Canteen

Commission for the Blind workers will be allowed access to the second floor to restock the machines in the canteen without an employee escort.

## IX. Meetings

In the event of a public meeting, an employee will be assigned to enable access to the elevator.

## X. Other

A copy of this policy shall be provided to employees with each ID badge issued and posted on the PEBA's Intranet.

# Information Assets Ethics and Use Policy

**THE LANGUAGE USED IN THIS DOCUMENT DOES NOT CREATE AN EMPLOYMENT CONTRACT BETWEEN THE EMPLOYEE AND THE AGENCY. THIS DOCUMENT DOES NOT CREATE ANY CONTRACTUAL RIGHTS OR ENTITLEMENTS. THE AGENCY RESERVES THE RIGHT TO REVISE THE CONTENT OF THIS DOCUMENT, IN WHOLE OR IN PART. NO PROMISES OR ASSURANCES, WHETHER WRITTEN OR ORAL, WHICH ARE CONTRARY TO OR INCONSISTENT WITH THE TERMS OF THIS PARAGRAPH CREATE ANY CONTRACT OF EMPLOYMENT.**

## Document control information

| | |
|---|---|
| **Office of responsibility** | Information Technology |

## Revision history

| | | | | | |
|---|---|---|---|---|---|
| **Revision** | 1 | **Approval date** | May 29, 2018 | **Section** | II, III, IV, VI |
| **Author** | James Manning | | | | |
| **Description of change** | • Removed reference to 8410.<br>• Updated language referring to PEBA's data classification scheme.<br>• Removed language defining specific disruptive internet use.<br>• Added language to prevent intentional actions to get around web filters.<br>• Changed "Computer worms and viruses" to malware. | | | | |
| **Revision** | | **Approval date** | | **Section** | |
| **Author** | | | | | |
| **Description of change** | | | | | |

# I. Scope

This policy applies to all South Carolina Public Employee Benefit Authority (PEBA) users. Its purpose is to: safeguard PEBA's assets, prevent software copyright infringement, and protect the integrity of the agency's computer environment.

## II. Information systems access

- Users are not granted access to any agency data until their supervisor requests the access.
- Access into PEBA's network, outside of the facility, is considered unauthorized if the access is without prior written authorization from the Administration and Information Technology departments.
- Upon a user's transfer or termination, the user's supervisor will ensure that the user's access to PEBA's data is terminated by contacting PEBA's Human Resources.
- Users are required to return to PEBA all agency assets (hardware, software or information) and other agency property in their possession or control upon termination or transfer of employment for employees, termination of engagement for non-employees, or immediately upon request.

## III. Confidentiality and privacy

- Users must keep confidential, unless otherwise exempted by federal or state statutes, all personal facts and health information made available to them during their employment.
- Users must acknowledge that their supervisors have informed them of the requirements of their positions regarding the type of protected information to which they have access in order to perform their assigned job duties.
- Users must make reasonable efforts to limit the access, use, and disclosure of, or requests for, protected health information to the minimum necessary to accomplish the intended purpose for which the use, disclosure or request is made.
- Users must make reasonable efforts to safeguard all personal facts and health information by following PEBA's privacy and security policies and procedures.
- All records of all active, retired, and inactive members of the retirement and insurance plans administered by PEBA are classified as confidential records and shall not be disclosed to third parties, except where authorized by the member, required by law, or authorized by the Executive Director in response to a request from state or federal authorities.
- Users who encounter information that is improperly labeled, in accordance with PEBA's data classification schema, shall consult with the owner of the information and/or the PEBA Information Security and/or Data Privacy team(s) to determine the appropriate data classification.
- Users must maintain the confidentiality of any confidential investment-related information received from the South Carolina Retirement System Investment Commission.
- Users must maintain the confidentiality of assigned access codes and passwords, must not disclose access codes or passwords to unauthorized personnel, and must take immediate action to change access codes or passwords if necessary.
- Any violation of PEBA's privacy and security polices resulting in inappropriate disclosure or release of information or violation of Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy and security regulations or South Carolina or federal statutes may result in disciplinary action up to and including termination of employment and may subject user to penalties under federal law.

- Any unauthorized disclosure or duplication of any of PEBA's information assets is contrary to this policy and may result in disciplinary action.

## IV. Use of licensed software and copyrighted material

- Users must use licensed software and vendor manuals according to vendor agreements entered into by the agency.
- Users are not permitted to install any software on PEBA's computers. The use of any unauthorized copies of software on PEBA's computers will not be tolerated.
- Users are not permitted to copy software from agency or vendor media, or any accompanying documentation or manuals, under any circumstances and are not permitted to install agency software on home or other computers.
- Users are not permitted to give licensed software to anyone outside of PEBA, including clients, contractors, and customers.
- All software used by the agency and on agency computers will be purchased through the proper procedures. Any such purchase must be approved by a user's supervisor, the department's executive manager, and the agency's information technology manager. Upon appropriate approval, information technology staff will purchase the software.
- All software must be installed by the agency's software manager or designee.
- Users who illegally reproduce software can be subject to civil and criminal penalties including fines and imprisonment.

## V. Personal use

- All personal computer and software configurations will be modified by information technology staff only.
- Users are not permitted to store personal files on PEBA's network computer systems. These files include, but are not limited to: pictures, music, movies, documents, and personal email messages.
- Any user who determines that there may be a misuse of information assets such as unauthorized duplication of software or a lapse in confidentiality of member, subscriber or retiree information must immediately notify his or her department manager, PEBA's Information Technology department, or PEBA's legal counsel.

## VI. Internet/email use

- Transferring state government commercial traffic, as well as research and educational traffic, is an acceptable use so long as such use is acceptable to all interconnected networks along the entire route from source to destination.
- The network shall not be used for illegal purposes or to support or assist such purposes. Examples of this would be the transmission of threatening, sexually explicit, obscene or otherwise illegal materials.

- Usage of the network should be prudent and should not disrupt network users, services and/or equipment, or substantially hinder others in their use of the network. Users should not take any intentional action to remove software from devices that are installed by the agency nor should users take any intentional actions to get around the agency's web filters. Other disruptions include, but are not limited to: distribution of unsolicited advertising; mass distribution of non-business related material; propagation of malware; unauthorized attempts to enter any other computer or network related devices; and sustained high volume network traffic.
- PEBA's computer systems and networks are to be used primarily for conducting official state business. It is recognized users may occasionally use these systems and networks for limited incidental personal use during non-working time. Such limited personal use may be acceptable as long as other usage policies are followed and the use does not interfere with a user's work or negatively impact the computer system or network, and does not result in additional public expense. These systems are not available or accessible for public speech or any First Amendment expressive activity or for use by the public. Further, the systems are expressly declared to not be a public forum.
- Users may be subject to limitations on their use of the network as determined by the appropriate supervising authority. PEBA reserves the right to control access to internet sites.
- Use of network services provided by PEBA may be subject to monitoring for security and/or other reasons. Any contents obtained under these guidelines may be disclosed without the consent of the user. Users of these services are therefore advised of this potential monitoring and agree to this practice.
- Any violation of the internet/email use policy may result in disciplinary action up to and including termination and may subject users to penalties under federal law.

## VII. Disciplinary action

Any violation of the *Information Assets Ethics and Use Policy* may result in disciplinary action up to and including termination and may subject users to penalties under federal law.

# S.C. Public Employee Benefit Authority

## News Media Contact and FOIA Request Policy and Procedures

Office of Responsibility: Communications Department
Revised: July 2017

**THE LANGUAGE USED IN THIS DOCUMENT DOES NOT CREATE AN EMPLOYMENT CONTRACT BETWEEN THE EMPLOYEE AND THE AGENCY, THIS DOCUMENT DOES NOT CREATE ANY CONTRACTUAL RIGHTS OR ENTITLEMENTS. THE AGENCY RESERVES THE RIGHT TO REVISE THE CONTENT OF THIS DOCUMENT, IN WHOLE OR IN PART. NO PROMISES OR ASSURANCES, WHETHER WRITTEN OR ORAL, WHICH ARE CONTRARY TO OR INCONSISTENT WITH THE TERMS OF THIS PARAGRAPH CREATE ANY CONTRACT OF EMPLOYMENT.**

# I. Policy statement

The South Carolina Public Employee Benefit Authority (PEBA) administers the state's employee insurance programs and retirement systems for South Carolina's public workforce. It is critical to PEBA's mission that the news media and public receive timely and accurate information about the activities of PEBA and its operations. The responsibility for providing information to the news media and public rests with the chairman of the PEBA Board of Directors, the executive director of PEBA, PEBA's chief operating officer and other designated individuals.

This policy applies to you in your official capacity as an employee of PEBA. This policy does not prohibit an employee from exercising his or her freedom of speech as a private citizen on matters of public concern.

Employees of PEBA are instructed to use extreme care to avoid disclosing any confidential or nonpublic information.

# II. News media contact

## A. General procedures

1. Employees of PEBA should refer the news media to PEBA's communications director.
2. It is the responsibility of the communications director, in conjunction with the executive director and chief operating officer, to determine who will provide information directly to the news media on individual issues.

3. Operational directors will be notified of non-routine requests for information from their areas of operations; requests which are non-controversial will be handled routinely as determined by the parties involved.
4. If PEBA's communications director is unavailable, employees should refer the news media to one of PEBA's public information directors.
5. If contact with the news media is unavoidable, employees should immediately report such contact to their supervisor and their operational director. PEBA's communications director should also be notified as soon as possible.
6. Employees should respond to requests from the communications director for information and/or access to PEBA divisions in an expeditious yet reasonable time frame.

### B. Interviews

1. All employee interviews with the news media should be arranged through PEBA's communications director. This includes print, broadcast, and online media interviews by telephone, through the internet, or in person.
2. Interviews of a personal nature (i.e., not related to job function or employee responsibilities) should not be conducted in any PEBA office/building at any time unless specific, prior permission has been granted by PEBA's executive director or chief operating officer.

***Exceptions:***

a. Occasionally, executive staff or a designee will be in a position to talk directly with the news media. Executive staff is defined as one of the following: executive director, chief operating officer, operational directors, and general counsel. Executive staff may also designate other managers to speak on the agency's behalf.
b. Executive staff should carefully consider the appropriateness of such direct contacts with the news media, bearing in mind that these discretionary decisions will vary from issue to issue. Sensitive matters affecting PEBA and its operations should always be referred to PEBA's communications director and/or PEBA's executive director and chief operating officer.
c. After contact with the news media, executive staff should notify PEBA's communications director immediately as to the subject matter and details thereof. Often, other media representatives may contact the communications director about the same issue and the Communications Department maintains a log of the agency's contact with the media.

## III. Freedom of Information Act (FOIA) requests

### A. General procedures

1. All requests for information pursuant to the South Carolina Freedom of Information Act (FOIA) should be forwarded upon receipt to PEBA's communications director, who will log in the request and either forward it to the appropriate area or

coordinate with executive staff to obtain the requested information if the information is available under FOIA.

2. All FOIA requests shall be answered in accordance with FOIA, including but not limited to time frames, definitions of releasable information, and exemptions. Matters not subject to disclosure under FOIA, or other state or federal law, will not be released. See Sections 30-4-10 et seq. of the *South Carolina Code of Laws* (1976) as amended.
3. If the communications director reasonably believes that a request involves matters exempt from disclosure under FOIA or other state or federal law, they will consult with PEBA's general counsel, or other PEBA attorney, prior to releasing the potentially exempt documents or records.
4. Non-PEBA employees shall not be allowed unsupervised access to PEBA premises or record files.
5. Prior to the release of records or information pertaining to the PEBA Board, PEBA employees, constitutional officers, or members and staff of the General Assembly, it is standard practice for PEBA's executive director or chief operating officer to inform the affected individuals concerning the FOIA request. This action should in no way be construed as circumvention of FOIA or compromising PEBA's intention to disclose information which is releasable under FOIA.
6. If the FOIA request is submitted by the news media, the communication's director, in conjunction with executive staff, shall determine who will provide FOIA information directly to the news media. All paper FOIA requests from the news media should be date stamped upon their receipt; if the FOIA request is received initially in an area other than the Communications Department, it should be date stamped at that location and immediately redirected to PEBA's communications director, at which time it will be date stamped again.
7. FOIA requests and responses must be in writing and be accompanied by a cover letter, even if the documents or records are delivered in person to the requestor. A formal response letter or email for each request must be retained in PEBA's FOIA files. Requests and responses under Section D of this policy are exempt from the requirements of this subsection.
8. All responses to FOIA requests that require a referral to another state agency must include a copy (and cc: on the response) to the agency to which the FOIA request is being referred. In addition, whenever possible, PEBA's communications director should contact the FOIA contact at the agency to which the FOIA request is being referred as a professional courtesy prior to the FOIA response being mailed to the requester.
9. No PEBA employee acting in his or her official capacity should submit a FOIA request to another governmental entity without prior approval of PEBA's executive director and/or chief operating officer.

## B. Final determination of public availability

1. Within 10 business days of receipt of a written request for records and documents under FOIA, the communications director must notify the person making the

request concerning PEBA's final determination concerning the public availability of the requested record. A "business day" does not include Saturdays, Sundays and legal public holidays.

2. If the requested information is more than 24 months old as of the date of the request, the communications director must notify the requester of PEBA's final determination concerning the public availability of the information within 20 business days (excluding Saturdays, Sundays and legal public holidays).
3. The final determination of public availability is not required to include a final decision, or express an opinion, as to whether specific portions of the documents or information may be subject to redaction under the exemptions of Section 30-4-40 or other state or federal law.
4. The deadlines for the final determination of public availability may be extended by the mutual agreement of PEBA and the requesting party. By law, this agreement is not to be unreasonably withheld. Section 30-4-30(C).
5. The communications director shall consult with appropriate PEBA employees to make the final determination concerning the public availability of requested documents and records. This includes, but is not limited to, researching files, pulling archived materials, copying information, developing a computer program or running an existing computer program, making records available for review, and seeking a legal opinion.
6. If information requested under FOIA is determined to be unavailable or non-releasable, PEBA's communications director shall provide written notification of PEBA's final determination, and the reasons thereof, within the 10-business-day or 20-business-day applicable time requirement of FOIA.
7. If PEBA fails to notify the requester of its final determination concerning the public availability of information within the 10-business-day or 20-business-day timeframe set out in Section 30-4-30(C), and there is no agreement to extend the deadline, the request is considered approved as to nonexempt records or information. FOIA exemptions set forth in Section 30-4-40 or other state or federal laws are not waived due to the agency's failure to provide the availability determination within the required timeframe.
8. With respect to FOIA requests for disclosure of employment applicant information the FOIA request shall be forwarded to the PEBA human resources director for processing in accordance with Section III(E) of this policy.
9. With respect to FOIA requests for information related to PEBA procurements, the FOIA request shall be forwarded to PEBA's procurement officer or procurement director for processing in accordance with Section III(F) of this policy.

## C. Response to approved FOIA request

1. If the communications director has granted or approved the FOIA request, the requested information must be furnished or made available for inspection and copying no later than 30 calendar days from the date of the final determination of public availability.

2. If the communications director has granted or approved a FOIA request of records older than 24 months at the time of the initial request, then the requested information must be furnished or made available for inspection and copying no later than 35 calendar days from the date of the final determination of public availability.
3. If, in accordance with Section III(G) of this policy, PEBA requires a deposit of up to 25 percent of the estimated cost of fulfilling a response to a request approved by the communications director, then the requested information must be furnished or made available for inspection and copying no later than 30 calendar days from the date PEBA received the deposit. If the records are more than 24 months old at the time of the request, then the record must be made available for inspection or copying no later than 35 calendar days from the date PEBA received the deposit. The full amount of the total cost must be paid at the time of production of the documents.
4. The response and production deadlines to fulfill a FOIA request may be extended by mutual agreement between PEBA and the requesting party. By law, this agreement shall not be unreasonably withheld. Section 30-4-30(C).
5. The general counsel, or other PEBA attorney, shall determine whether specific portions of documents in the approved FOIA request must be redacted according to exemptions in Section 30-4-40 or other state or federal law.
6. When requests involve a large amount of information, requestors should be given options for receiving the data. This could include allowing the requestor the opportunity to review disclosable records at PEBA offices rather than receiving hard or electronic copies if this will be more convenient for both parties. This step should be taken before PEBA staff begins assembling the data.
7. FOIA responses may be in paper or electronic format. If the request is made electronically, it is acceptable to respond in the same format. The requested information may be attached as a PDF or other comparable medium. Records must be provided in a form that is both convenient and practical for use by the requester.
8. PEBA may file a request for hearing with the circuit court to seek relief from unduly burdensome, overly broad, vague, repetitive, or otherwise improper FOIA requests. Section 30-4-110(A).
9. PEBA may also request a hearing with the circuit court if it is unable to make a good faith determination as to whether requested information is exempt from disclosure. Section 30-4-110(A).
10. The following text should be included in all responses to FOIA requests:

    a. *"Section 30-2-50 of the Code of Laws of the state of South Carolina provides that no person or private entity shall knowingly obtain or use any personal information obtained from a public body under FOIA for any commercial solicitation directed to a person in this state. The South Carolina Public Employee Benefit Authority, as a public entity, gives notice to you, as a requestor of records from this agency, that obtaining or using these public records for commercial solicitation is prohibited. Any person who knowingly uses public records for commercial solicitation is guilty of a misdemeanor and, upon conviction, must be fined an amount not to exceed five hundred dollars or*

*imprisoned for a term not to exceed one year, or both. Please see S.C. Code of Laws Section 30-2-10, et. seq. for full text of Family Privacy Protection Act."*

## D. FOIA request not required

1. A written FOIA request is not required for information that is immediately disclosable under the Act. This would include: 1) approved minutes of PEBA Board meetings and other committees for which PEBA provides staff support; and 2) all nonexempt documents reviewed by a PEBA Board member in a public meeting during the previous six months. S.C. Code Ann. Section 30-4-30(D).
2. The records enumerated above must be made available for public inspection and copying during PEBA's hours of operation unless the record is exempt pursuant to Section 30-4-40 or other state or federal law.

## E. Disclosure of employment applicant information

In accordance with the S.C. Freedom of Information Act (FOIA), S. C. Code § 30-4-10 et. seq. as amended, public bodies must make available to a requestor under FOIA the total number of applicants who applied for a specific employment position. In addition, public bodies must disclose all materials gathered during the employment search for not fewer than the final three applicants under consideration for any type of position.

### 1. Collection of applicant information

The following steps are to facilitate the processing of a FOIA request before it is received:

a. Designated contact to process Human Resources-related FOIA requests. PEBA's human resources director is the designated contact to process FOIA requests concerning applicant information. PEBA's human resources director is the designated custodian, and as such, ensures storage of and accessibility to all of this applicant information. All FOIA requests for applicant information should be forwarded to PEBA's human resources director, who will be responsible for all correspondence to and from the agency regarding those FOIA requests.

b. Determining the total number of applicants for a position. PEBA's human resources director shall maintain a current count of the number of applications that are accepted for an open position. Once the position is filled or applications are no longer being accepted for that position, the applications shall be grouped together, with the total number of applications accepted displayed clearly on an applicant log and maintained in the file folder in which the applications are kept.

c. Standard materials to gather concerning an applicant. The following is a list of materials that generally should be gathered for an applicant: application/resume, reference checks, and confirmation of salary for a state employee. Standardized information that must become part of the applicant's file shall be determined by the nature of the position.

d. Materials that may be gathered concerning an applicant. The following is a list of some materials to gather, dependent upon the specific position being filled: criminal background checks, credit checks, school transcripts, driver's license records, drug tests (including mandatory CDL drug testing), medical examinations, certification or licensing verifications, proficiency test scores (e.g., word processing and typing tests), writing samples, and interview notes.
e. Determining no fewer than the final three applicants for a position. Once all applications have been gathered for a position and all interviews have been completed, the hiring authority must identify no fewer than the final three applicants for the position and notify PEBA's human resources director on the Applicant Log form as to that identification.

## 2. FOIA request for applicant information

The following steps are to facilitate the processing of a FOIA request once it is received:

a. As set forth in Section III(B) above, PEBA's human resources director shall notify the requester of PEBA's final determination of public availability of the applicant information within the timeframe required by FOIA.
b. Assembling information to respond to the request. PEBA's human resources director will assemble all materials, regardless of their form or location, which were gathered in the search to fill the employment position.
c. Determining which information to disclose. PEBA's human resources director will determine which information to disclose under the FOIA request. The applicant's Social Security number, medical records, and tax information are exempt from disclosure by FOIA. Each FOIA request will be examined on a case-by-case basis for determining which information will be disclosed or not disclosed under the Freedom of Information Act. In determining what information to disclose under §30-4-40(a)(2) of FOIA, PEBA's human resources director should weigh the privacy interests of the applicant against the public's interest in disclosure. Depending on the specific situation, the following information should be evaluated to determine whether its disclosure would constitute an unreasonable invasion of personal privacy under § 30-4-40(a)(2): drug test results, unlisted phone numbers, salaries, criminal convictions, Family Independence Act (FIA) information, reasons for job terminations, credit check information, criminal background check information, reference letters, disability status, and driver's license numbers and records. Prior to the release of any information under this policy, PEBA's general counsel, or other PEBA attorney, will be consulted.
d. As set forth in Section III(C) of this policy, with respect to approved FOIA requests for employment applicant information, PEBA's human resources director will furnish information or produce documents for inspection and copying, or electronic transmission, within the timeframe and in the manner required by FOIA as set out in Section III(C).

## F. FOIA requests for procurement-related information

1. FOIA requests for information related to PEBA procurements pursuant to South Carolina Freedom of Information Act, including requests for proposals and solicitations, should be forwarded upon receipt to PEBA's procurement officer or procurement director.
2. As set forth in Section III(B) above, PEBA's procurement officer or procurement director shall notify the requestor of PEBA's final determination of public availability of requested procurement information within the timeframe required by FOIA.
3. As set forth in Section III(C) of this policy, with respect to approved FOIA requests related to PEBA procurements or solicitations, PEBA's procurement officer or procurement director will furnish information or produce documents for inspection and copying, or electronic transmission, within the timeframe and in the manner required by FOIA.

## G. Charges for FOIA requests

1. FOIA requests should be answered without charge, or at a reduced charge, when the request will benefit the public interest and requires minimal and/or a reasonable amount of employee time and photocopying expense.
2. For requests which require substantial employee time for searching and/or photocopying, etc., a reasonable charge may be assessed on the person or organization requesting the information. FOIA requests which involve computer programs/runs will also be assessed a reasonable charge.
3. Guidelines for determining what is reasonable are established for PEBA as follows:
   a. Photocopying - if the FOIA request requires copying approximately *50 pages or more* at one time or a similar amount over several days, the charge would be calculated at *5 cents per page*;
   b. Employee/administrative time - if the FOIA request requires approximately *one hour or more* of staff time for the search, retrieval, or redaction of records, the charge will be based on the *hourly wage* of the employee(s) responding to the request. The staff member assigned to the FOIA request will be the lowest paid employee who, in the reasonable discretion of the custodian of the records, has the necessary skills and training to perform the request.
   c. Postage or fax - if the FOIA request requires postage or a fax expense of approximately *$2.00 or more*, the charge would be the *actual cost* associated with the process.
   d. Computer time - if the FOIA request requires development of a computer program or running an established program, the charge would be based on *costs associated with the process*.
4. Members of the General Assembly shall receive copies of records or documents at no charge when their request relates to their legislative duties.
5. Copy charges do not apply to records that are transmitted in an electronic format.
6. If records are not in an electronic format and PEBA agrees to produce them in an electronic format, PEBA will charge the reasonable cost associated with the process.

The reasonable charge shall be in accordance with the "Employee/administrative time" and "Computer time" paragraphs set out above.

7. Fees shall not be charged for examination and review to determine if documents are subject to disclosure.
8. Any individual making a FOIA request which will result in a charge shall be notified in advance of the approximate cost for providing that information; notification and acceptance of those charges must be in writing (paper or email).
9. Payment in part or in full for a FOIA request may be required by PEBA prior to the release of any records. If the cost of responding to the request is estimated to be *$200 or more*, then a minimum deposit amounting to *at least 25 percent of the total reasonably anticipated cost* will be required prior to PEBA searching for or making copies of records. Requests for payment in advance shall be in writing.
10. Payment for FOIA requests should be made payable to PEBA. Checks/money orders should be forwarded to PEBA's communications director, who will ensure that payment is delivered to PEBA's accounts payable staff with notation as to which account into which the payment should be deposited. Payment will be deposited and credited to the operational or administrative area that provided the response to the FOIA request. Constitutional officers, members of the General Assembly, and other state agencies shall not be charged for information or records released under FOIA.
11. Charges may be waived or levied at the discretion of PEBA's executive director and/or chief operating officer.

# S.C. Public Employee Benefit Authority

## Physical Safety and Security Plan

Office of Responsibility: Risk and Compliance
Revised: September 2017
Approved: 9/26/2017

**THE LANGUAGE USED IN THIS DOCUMENT DOES NOT CREATE AN EMPLOYMENT CONTRACT BETWEEN THE EMPLOYEE AND THE AGENCY, THIS DOCUMENT DOES NOT CREATE ANY CONTRACTUAL RIGHTS OR ENTITLEMENTS. THE AGENCY RESERVES THE RIGHT TO REVISE THE CONTENT OF THIS DOCUMENT, IN WHOLE OR IN PART. NO PROMISES OR ASSURANCES, WHETHER WRITTEN OR ORAL, WHICH ARE CONTRARY TO OR INCONSISTENT WITH THE TERMS OF THIS PARAGRAPH CREATE ANY CONTRACT OF EMPLOYMENT.**

### I. Emergency Contact Information

| Type of Emergency | Phone Number |
|---|---|
| Fire | 911 |
| Medical Emergency | 911 |
| Weather Emergency | 911 |
| Bomb Threat/Suspicious Package | 803.734.2422 (Day)<br>803.734.8700 (Night) |
| Theft | 803.734.2422 (Day)<br>803.734.8700 (Night) |
| Personal Safety/Suspicious Person | 803.734.2422 (Day)<br>803.734.8700 (Night) |
| Building Emergency (202 Arbor Lake) | 803.734.3308 (General Services)<br>803.261.9571 (James Manning)<br>803.315.0627 (Travis Turner) |
| Building Emergency - CBRE (200 Arbor Lake) | 803.744-6854<br>803.518.9172 |
| USC Fire Alarm | 803.777-4215 |
| Building Alarm | 803.667.5959 (Alvin Carpenter)<br>803.413.6631 (Robby Brown) |
| Domestic Violence | 803.734.2422 |
| | |
| | |
| | |

## II. Visitors

Individuals who are not employees of PEBA but are engaged in work activities at PEBA's facility are required to sign in at the receptionist desk.

Visitors to PEBA must be escorted by an employee when on PEBA premises. Visitor badges will be provided and will be issued at the receptionist desk. Before visitors leave PEBA premises, visitor badges are to be returned to the receptionist. Visitors going to the canteen should be escorted by an employee. Visitors needing access beyond the first floor will be met at the elevator and escorted by an employee from the area to which they need access.

Employees are asked to not allow visitors to enter the building at any time other than the PEBA's core business hours of 8:30 a.m. to 5:00 p.m.

Employees may use the back entrance to the building to avoid after-hours contact with visitors.

## III. Fires and Fire Alarms

A. If you see smoke, or see flames, or smell something burning, or hear see/hear the fire alarm, **Immediately**:
   a. **Isolate** the Fire (close the door if you can do safely).
   b. **Call** 911 and activate the fire alarm.
   c. Initiate pre-recorded message on intercom system

d. **Evacuate** using the nearest exit/stairs that is safe to use and exit the building as quickly as possible. If you are in a location with a door, please close the door behind you. Meet at the designated assembly area close to Arbor Lake Drive.
e. **Fire Extinguishment** is optional once all of the steps above have been initiated.

B. Persons in Need should wait at the top of the stairwells for assistance.
C. Floor wardens will search their assigned areas to ensure people have fully evacuated and to assist people to the nearest safe exit.
D. Accountability monitors will be located at the assembly area to assist managers in determining if people are missing.
    a. When visitors are in the building, the staff member responsible for the visitor has the responsibility of accounting for their visitor(s).
E. Do not re-enter the building until advised by the fire Bureau.
F. The Bureau of Public Safety Officer assigned to PEBA will place orange cones in the parking lot to redirect traffic.

## IV. Medical Emergencies

A. If you find a person who has a true medical emergency, immediately:
    a. **Call** 911.
    b. **Do not move** the victim unless safety dictates.
    c. **Use pressure**, if trained, to stop bleeding.
    d. **Use CPR**, if trained, if no pulse and not breathing.
    e. **Use the AED**, if trained and medical emergency requires it
    f. **Clear the area** to ensure safety and privacy.
    g. **Alert Human Resources** as soon as possible.
    h. **Document information** such as name of the victim, location of the injury, cause of the injury, etc.

B. If you find a person who has an injury that does not represent a true medical emergency:
    a. **Do not move** the victim unless safety dictates.
    b. **Clear the area** to ensure safety and privacy.
    c. **Use pressure**, if trained, to stop bleeding.
    d. **Alert Human Resources** as soon as possible to get instructions on how to proceed.

C. AEDs are maintained in accordance with the manufacturer's recommendation as well as in accordance with State and Federal Law. There is at least one AED on each floor that is located in an obvious location.

D. PEBA will have at least one staff member on each floor trained to give first aid, perform CPR, and to use the AED's.

E. First aid kits are located in the same location as the AED devices. Human Resources also has a first aid kit available.

## V. Storm/Weather Emergency

A. Tornado / Hurricane / High Winds
    a. Stay indoors.
    b. Move away from windows and open doors (preferably into an interior hallway).

c. If possible, move to the lowest level of the building.
d. Do not use elevators, electrical equipment or telephones.
e. Sit on the floor and cover your head with your arms to protect yourself from flying debris.
f. Do not leave the building. Visitors will be made aware of the situation and will be accommodated if they wish to follow agency protocols.
g. Initiate pre-recorded message on intercom system
h. Await instructions from emergency management officials.

B. Earthquake
   a. Stay indoors.
   b. Crawl under a table or desk or brace yourself by standing in an interior doorway.
   c. Do not use elevators, electrical equipment or telephones.
   d. Do not use open flame.
   e. Be prepared for aftershocks.
   f. Do not leave the building. Visitors will be made aware of the situation and will be accommodated if they wish to follow agency protocols.
   g. Await instruction from emergency management officials.

C. Floods
   a. Stay indoors.
   b. Never attempt to walk or drive through flood waters.
   c. Await instructions from emergency management officials.

D. Winter Storms
   a. Stay indoors.
   b. Do not walk or drive during the storm and risk becoming stranded.
   c. Await instructions from emergency management officials.

E. Agency Closings and Cancellations
   a. Section 8-11-57 of the S.C. Code of Laws, as amended, **authorizes the Governor to declare a state of emergency or order all or some state offices closed** due to hazardous weather conditions and authorize up to five days leave with pay for affected state employees who are absent from work due to the state of emergency or the hazardous weather conditions. As the possibility of winter weather hazards increase, please remember that, based on the decision of the Office of the Governor and the Emergency Management Division, **State government offices and their employees will follow the same winter weather hazard decisions made by the county government officials where the state office is located.** For example, a county's decision to delay opening or close county government offices would mean state employees who work in the impacted county would also delay opening or close state government offices. A delay opening or closing of our agency will be based upon the decision of whether Richland County Government has a delayed opening or closing.

      The South Carolina Emergency Management Division will post the most recent closing/delay information on their website at www.scemd.org/closings.

## VI. Bomb Threat/Suspicious Package

**A. If a bomb threat is received by phone:**

1. Remain calm. Keep the caller on the line for as long as possible. DO NOT HANG UP, even if the caller does.
2. Listen carefully. Be polite and show interest.
3. Try to keep the caller talking to learn more information.
4. If possible, write a note to a colleague to call the authorities or, as soon as the caller hangs up, immediately notify them yourself.
5. If your phone has a display, copy the number and/or letters on the display.
6. Complete the Bomb Threat Checklist immediately. Write down as much detail as you can remember. Try to get exact words.
7. Immediately upon termination of the call, do not hang up, but from a different phone, contact the Bureau of Public Safety immediately with information and await instructions.

**B. If a bomb threat is received by handwritten note:**

1. Call DPS 803.734.2422
2. Handle note as minimally as possible.

**C. If a bomb threat is received by email:**

1. Call DPS 803.734.2422
2. Do not delete the message.

**D. Signs of a suspicious package:**

1. No return address
2. Restrictive Markings
3. Sealed with tape
4. Misspelled words or badly typed or written
5. Unknown powder or suspicious substance
6. Excessive Postage
7. Stains or discolorations
8. Strange odor
9. Incorrect title or addressed to title only
10. Rigid or bulky
11. Lopsided/Uneven or unusual weight
12. Protruding wires

**DO NOT:**

- Use two-way radios or cellular phone; radio signals have the potential to detonate a bomb.
- Evacuate the building until police arrive and evaluate the threat.
- Activate the fire alarm.
- Touch or move a suspicious package.
- Open, smell or taste the package.
- If you have been exposed to a chemical threat – do not leave the area

**DO:**

- Isolate the package immediately
- Leave the area where the package is located (Do not exit the building)
- Close any doors and prevent others from entering the area
- Wash your hands with soap and water
- Notify the Bureau of Public Safety and your supervisor

## VII. Suspicious person or staff member feels threatened

A. If a suspicious person is identified on the premises call the Bureau of Protective Services immediately and alert your supervisor.
B. If a PEBA staff member feels threatened they should call the Bureau of Protective Services immediately. Staff members with a panic button should activate that device. If possible, staff should remove themselves from the situation and also alert their supervisor as soon as possible.

## VIII. Lockdown

**A.** In the event that there is imminent danger in the immediate area, the facility can be placed into lockdown.
**B.** All staff should remain in the building. Visitors will be made aware of the situation and will be accommodated if they wish to follow agency protocols.
**C.** Staff and visitors will be allowed to enter the building.
**D.** BPS will coordinate with other local authorities as necessary.
E. Initiate pre-recorded message on intercom system

## IX. Active Shooter

A. Call 911 and alert the police to the shooter's presence and location. If you can't speak, leave the line open so the dispatcher can listen.
B. Initiate pre-recorded message on intercom system.
C. Visitors will be made aware of the situation and will be accommodated if they wish to follow agency protocols.
D. **RUN** – If you feel that you can safely exit the building, do so with the following in mind:
    a. Make sure you have an escape route in mind
    b. Do not carry anything with you
    c. Move quickly and quietly
    d. There will be no assembly area outside, keep moving to a safe location
    e. If you encounter emergency personnel, keep your hands visible and follow their commands
E. **Hide** – If you can't safely exit the building, then hide where you feel you will be undetected and safe from the intruder
F. **Fight** – If you cannot escape, you can overpower the intruder as a **Last Resort**.
G. Do not attempt to move injured people. Tell authorities of their location.

## X. Parking Lot Safety

A. DPS will patrol the parking lot area in their vehicle from 4:30 until 5:30 to ensure the safety of staff when leaving work.
B. PEBA staff may request that a DPS officer escort them to their vehicle when leaving work by calling the DPS dispatch number or by stopping by direct request to the DPS officer on duty.

south carolina peba SM
state health plan | retirement systems

*Serving those who serve South Carolina*

# S.C. Public Employee Benefit Authority

## Social media policy for agency employees

Office of Responsibility: Communications
Revised: January 2017

**THE LANGUAGE USED IN THIS DOCUMENT DOES NOT CREATE AN EMPLOYMENT CONTRACT BETWEEN THE EMPLOYEE AND THE AGENCY, THIS DOCUMENT DOES NOT CREATE ANY CONTRACTUAL RIGHTS OR ENTITLEMENTS. THE AGENCY RESERVES THE RIGHT TO REVISE THE CONTENT OF THIS DOCUMENT, IN WHOLE OR IN PART. NO PROMISES OR ASSURANCES, WHETHER WRITTEN OR ORAL, WHICH ARE CONTRARY TO OR INCONSISTENT WITH THE TERMS OF THIS PARAGRAPH CREATE ANY CONTRACT OF EMPLOYMENT.**

Online social networks such as Twitter, Facebook, YouTube and LinkedIn can be valuable tools for communicating with the stakeholders. The South Carolina Public Employee Benefit Authority (PEBA) encourages the appropriate development and deployment of these communications methods.

### I. Guidelines for all PEBA employees

PEBA employees should be sensitive to the fact that social networks and other online forums like blogs, live messaging/chat sessions, and online video conferencing blur the distinction between an individual's professional and personal lives. PEBA encourages employees to apply the same common-sense principals and guidelines that the agency uses for appropriate use of all company property, such as telephones, personal computers, or photocopiers. Social media usage differs in that it extends to outside of the office and after business hours. Inappropriate use of social media at any time can harm the agency's reputation, and yours. Here are some common sense guidelines to help you determine what the agency considers appropriate social media use with regard to topics that pertain to the agency and its operations. This list is not exclusive.

1. Remember that your posts and comments are public and may be seen by a lot of people.
2. Give your online posts and comments the same consideration you would give to comments you would make in a meeting or other public forum.
3. For PEBA employees, this includes confidential information, such as personal health information and personally identifiable information. If you need a reminder of what information falls within these categories, please refer to the agency's Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Manual.

4. Be mindful that some information posted by others may be protected by copyright and privacy laws. Sharing this information may violate those laws.
5. Practice common courtesy and treat others with respect online and in the physical workplace.
6. If your personal social media presence reflects who you work for and you post a comment that relates to your employer, please be clear that the views you are expressing are your own.
7. Always think twice before posting or commenting on social media networks. Ask yourself if you would be okay with your manager or an agency senior leader seeing the post or comment.
8. Never use or refer to your formal position when writing in a non-official capacity. Do not use your official email to establish a private social media or blog presence.
9. To others online, there is no clear distinction between your work life and your personal life. Always be honest and respectful in both capacities.

## II. Additional guidelines for PEBA employees managing the agency's social media programs

In addition to the guidelines for all PEBA employees, the following apply to PEBA employees who manage any of the agency's online presences as part of their job responsibilities.

1. Submit all posts and comments to the communications director for prior approval.
2. Submit posts or comments involving sensitive subject matter to the appropriate senior leaders for prior approval.
3. Make the communications director and/or senior leaders aware of posts and comments as necessary and appropriate.
4. Ensure that all agency posts and comments reflect PEBA's commitment to accountability, transparency and superior customer service.
5. Do not approve any posts that contain an individual's personal health information or personally identifiable information. The agency's Facebook Policy includes provisions for protecting a user's PHI and PII from disclosure by keeping a post hidden from the agency's Facebook page timeline. Make every effort to contact the user to let him know why his post will not be approved and quote the privacy portion of the agency's Facebook policy.
6. On your personal social media networks, be sure to represent only yourself, not the agency.
7. When posting or commenting in your official capacity, do not write anything that could appear to be legal advice. Legal issues should be handled through PEBA's Legal

Department to avoid conflicts and other ethical problems.

8. Emails and other correspondence conducted over personal social media channels that is official business of PEBA should be preserved and retained in a manner similar to other official documents. If you receive an unsolicited official contact through your personal email or social media presence, forward a copy of the correspondence to your official email account and respond from that platform.

   If you are responding on a non-PEBA site concerning an official PEBA matter, be sure to identify yourself and your position with PEBA. Comment only about matters that you are qualified to address. Do not respond without first consulting with your supervisor or the communications director.

# S.C. Public Employee Benefit Authority

## Tobacco-Free Workplace Policy

Office of Responsibility: Human Resources
Effective: June 1, 2017

**THE LANGUAGE USED IN THIS DOCUMENT DOES NOT CREATE AN EMPLOYMENT CONTRACT BETWEEN THE EMPLOYEE AND THE AGENCY, THIS DOCUMENT DOES NOT CREATE ANY CONTRACTUAL RIGHTS OR ENTITLEMENTS. THE AGENCY RESERVES THE RIGHT TO REVISE THE CONTENT OF THIS DOCUMENT, IN WHOLE OR IN PART. NO PROMISES OR ASSURANCES, WHETHER WRITTEN OR ORAL, WHICH ARE CONTRARY TO OR INCONSISTENT WITH THE TERMS OF THIS PARAGRAPH CREATE ANY CONTRACT OF EMPLOYMENT.**

### I. Policy Statement

The SC Public Employee Benefit Authority is committed to the well-being of our employees, customers, and visitors. In accordance with our commitment to promoting and protecting the health of our employees, all PEBA offices will be completely tobacco-free workplaces. The intent of this policy is to create an environment that promotes tobacco prevention, eliminates the risks associated with secondhand smoke, and is conducive to quitting the use of tobacco. Compliance with this policy is the responsibility of all PEBA employees.

### II. Covered Individuals

The provisions of this policy apply 24 hours a day, seven days a week to all employees, customers, contractors, vendors, and visitors.

### III. Definitions

A. *Tobacco and smoking products* include all products that are tobacco-derived or contain tobacco, including but not limited to cigarettes, electronic cigarettes, cigars, cigarillos, pipes, water pipes, smokeless tobacco products (chew, pouches, snuff), or any device intended to simulate smoked tobacco. This does not include nicotine replacement therapy, such as nicotine gum, patches, and lozenges.

B. *PEBA's workplace* includes any and all 200 and 202 Arbor Lake Drive property, including all buildings, facilities, grounds, common areas, sidewalks, and parking lots associated with either building, regardless of whether signs are posted or not.

## IV. Use of Tobacco Products

A. The use of tobacco and smoking products is prohibited at PEBA workplaces. No ashtrays, receptacles, or smoking shelters will be permitted.

B. The use of tobacco and smoking products is prohibited in PEBA-owned, operated, or leased vehicles.

C. PEBA discourages the use of tobacco and smoking products by all covered individuals on properties adjacent to PEBA workplaces.

## V. Communication of Policy

This policy will be communicated to PEBA employees, customers, and visitors as follows:

- News and information related to this policy will be posted on the agency website and intranet.
- References to this policy will be added to new employee orientation materials and other publications as appropriate.
- Self-identified tobacco users will be referred to the S.C. Tobacco Quitline at 1-800-QUIT-NOW.
- PEBA staff may assist in informing visitors of the policy and ask that they comply while at any PEBA workplace.
- Tobacco-free signs will be posted where appropriate.

## VI. Tobacco Cessation Resources

PEBA will offer resources and support to assist those tobacco users who desire to quit or abstain from using tobacco. Tobacco cessation resources and programs will be promoted or offered to PEBA employees and customers. Many of these programs are offered at little or no cost. Referrals may be made to the S.C. Tobacco Quitline at 1-800-QUIT-NOW.

## VII. Enforcement and Compliance

A. Compliance with the policy is the responsibility of every PEBA employee. Employees are expected to assume leadership roles by adhering to the policy provisions.

B. PEBA employees may address violations of this policy as described in the provisions below.

1. Violations by PEBA employees, contractors, and vendors should be reported to and handled by Human Resources.

2. Violations by customers and visitors may be addressed by any PEBA employee in a civil and respectful manner. Repeated violations or refusals to comply may be directed to the Visitor Intake department.

C. Corrective actions may include an educational component and, for those who wish to quit using tobacco, referral to a tobacco cessation program. Referrals may be made to the S.C. Tobacco Quitline at 1-800-QUIT-NOW.

D. Violations of this policy by PEBA employees may result in disciplinary action in accordance with the Progressive Discipline Policy.

# S.C. Public Employee Benefit Authority

## Workplace Violence Policy

Office of Responsibility: Human Resources
Revised: March 2013

**THE LANGUAGE USED IN THIS DOCUMENT DOES NOT CREATE AN EMPLOYMENT CONTRACT BETWEEN THE EMPLOYEE AND THE AGENCY, THIS DOCUMENT DOES NOT CREATE ANY CONTRACTUAL RIGHTS OR ENTITLEMENTS. THE AGENCY RESERVES THE RIGHT TO REVISE THE CONTENT OF THIS DOCUMENT, IN WHOLE OR IN PART. NO PROMISES OR ASSURANCES, WHETHER WRITTEN OR ORAL, WHICH ARE CONTRARY TO OR INCONSISTENT WITH THE TERMS OF THIS PARAGRAPH CREATE ANY CONTRACT OF EMPLOYMENT.**

### I. Policy

The SC Public Employee Benefit Authority has a zero tolerance policy regarding any type of harassment, intimidation, or workplace violence committed by or against employees or members of the public. The Agency is committed to providing a safe and healthy work environment.

### II. Prohibited Conduct

Employees are prohibited from making threats or engaging in violent activities. Examples of prohibited conduct may include but are not limited to:

- Physical – the use of force in order to harm
- Threats – expressions of intent to inflict injury
- Harassment – words, gestures and actions which tend to alarm, abuse, trouble or worry another person
- Property Damage – intentional damage to property owned or leased by the state, employees, visitors or vendors
- Weapons – weapons of any kind are prohibited on premises and in possession of an employee during work time (exception for law enforcement)

### III. Reporting Procedures

Employees should call 911 for all emergency situations before calling designated officials. Any dangerous or potentially dangerous situations should be reported immediately to a supervisor or Human Resources. Supervisors receiving a complaint or who has reason to suspect violence, threats or harassment must notify Human Resources immediately.

All reported incidents will be investigated. Investigations will be conducted confidentially to the extent possible and information will be disclosed to others only on a need-to-know basis. Parties involved in a situation will be provided the appropriate assistance and resources and will be apprised of the results of the investigation.

## IV. Prevention

Hiring – The Agency will conduct criminal background checks to reduce the risk of hiring individuals with a history of violent behavior.

Safety – Supervisors should regularly review the workplace to evaluate and identify any vulnerability to workplace violence or hazards. Necessary corrective action will be taken to reduce risks.

Awareness – While employees are not expected to be skilled at identifying potentially dangerous persons, they are expected to exercise good judgment and to inform Human Resources if they are aware of behavior which could be a sign of a potentially dangerous situation – such behavior includes:

- Obsession with weapons or bringing them to the workplace
- Displaying overt signs of extreme stress, resentment, hostility or anger
- Making threatening remarks
- Sudden or significant deterioration of performance
- Displaying irrational or inappropriate behavior
- Domestic violence situations

## V. Enforcement

Threats, threatening conduct, or any other acts of aggression or violence in the workplace will not be tolerated. Any employee determined to have committed such acts will be subject to disciplinary action up to and including termination. Non-employees engaged in violent acts on the employer's premises will be reported to the proper authorities.

## 6.2. Security Awareness Training

| | |
|---|---|
| Purpose | The purpose of security and awareness training is to define the information security training requirements for PEBA employees, contractors and third party users. |
| Policy | Security Awareness Training and Information Security Workforce<br>6.2.1. PEBA management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.<br>Role-Based Security Training<br>6.2.2. PEBA shall impart appropriate awareness training and regular updates in organizational policies and procedures to all employees of the organization and to, contractors and third party users, as relevant for their job function.<br>6.2.3. Training must be accompanied by an assessment procedure based on the cyber security training content presented in order to determine comprehension of key cyber security concepts and procedures.<br>6.2.4. Access to PEBA information assets and systems will be authorized for those users whose cyber security awareness training is current (e.g., having passed the most recent required training stage).<br>Testing, Training, and Monitoring<br>6.2.5. PEBA will appoint a cyber-security awareness training coordinator to manage training content, schedules and user training completion status.<br>6.2.6. The PEBA cyber security training coordinator, along with the agency Security Officer will review training content on an annual basis to ensure that it aligns with State of South Carolina policies.<br>6.2.7. The HIPPA Exam will be administered to all PEBA employees within 30 days of start of employment. |
| Guidance | NIST SP 800-53 Revision 4: AT 2 Security Awareness Training<br>NIST SP 800-53 Revision 4: AT 3 Role-Based Security Training<br>NIST SP 800-53 Revision 4: PM 13 Information Security Workforce<br>NIST SP 800-53 Revision 4: PM 14 Testing, Training, and Monitoring<br>**HIPAA Security Regulations Citations:**<br>45 CFR 164.308(a)(3) Workforce Security (R) |

## 7.3. System Development and Maintenance

**Purpose**

The purpose of the system development and maintenance section is to define requirements for system security planning and to improve protection of PEBA information system resources.

**Policy**

System Security Plan

7.3.1. PEBA shall prepare system security plans and documentation for critical enterprise information systems or systems under development.

7.3.2. System security plans shall provide an overview of the security requirements of the system and describe the controls in place for meeting the requirements through all stages of the systems development life cycle.

7.3.3. When the system is modified in a manner that affects security, system documentation shall be updated accordingly.

Vulnerability Scanning

7.3.4. PEBA shall perform a vulnerability assessment on all enterprise information systems undergoing significant changes, before the systems are moved into production.

7.3.5. PEBA shall perform periodic vulnerability assessments on production enterprise information systems and take appropriate measures to address the risks associated with any identified vulnerabilities.

7.3.6. Vulnerability notifications from vendors and other appropriate sources shall be monitored and assessed for all information systems and applications.

System and Services Acquisition Policy and Procedures

7.3.7. PEBA shall develop and follow a set of procedures consistent with State procurement standards as defined by the Information Technology Management Office.

7.3.8. PEBA shall ensure that the State's interests have been protected and enforced in all IT procurement contracts.

System Development Life Cycle

7.3.9. PEBA shall implement appropriate security controls at all stages of the information system life cycle

External Information System Services

7.3.10. PEBA shall supervise and monitor outsourced software development to validate PEBA security requirements.

Developer Security Testing and Evaluation

7.3.11. PEBA shall establish separate development, testing, and production environments

Development Process, Standards, and Tools

7.3.12. PEBA shall approve, document, and control the use of live data for use in preproduction environments and ensure that appropriate safeguards are in place to protect the data to the

same extend as the data is protected in the production environment.

Flaw Remediation

7.3.13. PEBA shall design appropriate controls into information systems, including user developed applications to ensure correct processing.

7.3.14. PEBA shall ensure that software patches are applied when they function to remove or reduce security weaknesses (see Appendix 7).

Security Alerts, Advisories, and Directives

7.3.15. PEBA shall collect information system security alerts, advisories, and directives on patches on an ongoing basis and implement these security directives in accordance with established time frames.

7.3.16. The Security Administrator monitoring vulnerabilities and vendors' releases of patches and fixes.

Software, Firmware, and Information Integrity

7.3.17. PEBA shall ensure that any decision to upgrade to a new release shall take into account the business requirements for the change, and the security of the release (e.g., the introduction of new security functionality or the number and severity of security problems affecting this version).

7.3.18. PEBA shall test critical operating system (OS) changes and updates in the test environment to ensure there is no adverse impact on organizational operations or security.

Information Input Validation

7.3.19. PEBA shall incorporate controls into information systems to check the validity of information inputs and information outputs.

7.3.20. PEBA shall incorporate processing validation checks into information systems to detect processing errors, inadvertent or deliberate processing actions (e.g., accidental deletions).

Session Authenticity

7.3.21. PEBA shall identify the appropriate controls to ensure session authenticity, protecting message integrity in applications and protecting information transmission to and from information systems.

| | |
|---|---|
| Guidance | NIST SP 800-53 Revision 4: PL 2 System Security Plan<br>NIST SP 800-53 Revision 4: RA 5 Vulnerability Scanning<br>NIST SP 800-53 Revision 4: SA 2 System and Services Acquisition Policy and Procedure<br>NIST SP 800-53 Revision 4: SA 3 System Development Life Cycle<br>NIST SP 800-53 Revision 4: SA 9 External Information System Services<br>NIST SP 800-53 Revision 4: SA 11 Developer Security Testing and Evaluation<br>NIST SP 800-53 Revision 4: SI 2 Flaw Remediation<br>NIST SP 800-53 Revision 4: SI 7 Software, Firmware, and Information Integrity<br>NIST SP 800-53 Revision 4: SI 10 Information Input Validation<br>NIST SP 800-53 Revision 4: SC 23 Session Authenticity |
| Reference | http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx |

# Data Classification Schema with Guidance and Examples

## DATA CLASSIFICATION SCHEMA

This Data Classification Schema has been developed to categorize the types of data that the SC Public Employee Benefit Authority (PEBA) possesses. PEBA must understand the types of information it uses and holds, and establish appropriate information handling procedures in order to prevent the unauthorized use or disclosure of sensitive information.

## Data Classification Objectives

1. Define consistent handling procedures for PEBA data based on risk
2. Facilitate decision making
3. Facilitate employee training and understanding
4. Define consistent IT implementation guidelines
5. Remain compliant with federal, state, and PEBA Information security and privacy policies

## PEBA data classification schema Levels

1. **Public information:** Information that is intended to be shared with the public.
2. **Internal use:** Non-sensitive information that is used in the operations of an agency.
3. **Confidential:** Sensitive information that is used or held by an agency. Loss or harm could occur as a result of unauthorized access, use, or disclosure of this information. Statutory or regulatory penalties, notification provisions, or other mandates could result if the information is accessed, used or disclosed in an unauthorized manner.
4. **Restricted:** Highly sensitive information that is used or held by an agency. For PEBA this primarily represents medical data and information pertaining to specific protected classes of individuals (i.e. children).

**Examples of Information by Data Classification Level**

| RESTRICTED | CONFIDENTIAL | INTERNAL USE | PUBLIC INFORMATION |
|---|---|---|---|
| • Medical data including claims and diagnoses<br>• National Medical Support Notice data<br>• Disability retirement medical review data<br>• Medicare reason code for N-stage renal failure<br>• Child welfare and legal information about minors (juvenile justice, foster care and/or adoption) | • Protected Health Information (HIPAA/HITECH)<br>• Pension/Retirement benefit information (actual amounts)<br>• Social Security numbers<br>• Date of birth<br>• Bank account numbers<br>• Debit or credit card numbers<br>• Driver's license information or State identification card information<br>• Employer Identification Number (EIN) of a sole proprietor<br>• Personal demographics (race, place of birth, weight, religion)<br>• Federal tax information (IRS Pub. 1075)<br>• Security plans, network architecture, etc.<br>• Unpublished information about agency personnel<br>• Photographs of individual people<br>• Information received from and/or about a business (tax information, business plans)<br>• Passport numbers<br>• Individual financial information subject to Gramm-Leach-Bliley Act (GLBA)<br>• Student education records<br>• Passwords | • Agency policies, procedures, and standards<br>• Internal training materials<br>• Internal meeting information<br>• Aggregated and de-identified data<br>• Operational performance data<br>• Procurement and contract data | • Public website content<br>• Publicly distributed information<br>• Meeting agendas and minutes from public meetings<br>• Brochures<br>• Public presentation materials<br>• Press releases<br>• Agency contact information |