

MANAGEMENT DIRECTIVE

Commonwealth of Pennsylvania Governor's Office

Subject: Maintenance, Access, and Release of Employee Information	Number: 505.18 Amended
Date: September 23, 2014	By Direction of:  Kelly Powell Logan, Secretary of Administration
Contact Agency: Office of Administration, Office for Human Resources Management, Human Resources Service Center, Telephone 717.787.8001	

This directive establishes policy, responsibilities, and procedures for the maintenance, access, and release of employee information. Marginal dots are excluded because of major changes to the directive.

1. **PURPOSE.** To establish policy and procedures for the maintenance, access, and release of employee information, other than Right to Know Law (RTKL) requests.
2. **SCOPE.** This directive applies to all state agencies, departments, boards, and commissions under the Governor's jurisdiction.
3. **OBJECTIVES.**
 - a. To provide a uniform system of maintaining, accessing, and releasing employee information.
 - b. To preserve and protect the privacy of all current and past employee information.
4. **DEFINITIONS.** The following definitions pertain to this directive. For purposes other than this directive, these words and terms may have different meanings.
 - a. **Access.** The ability to examine Confidential Employee Information (CEI). Examining such information includes, but is not limited to, accessing email, the agency's shared drive or resource accounts and obtaining the key to a locked security device.
 - b. **Agency Human Resource (HR) Records Custodian.** The HR Director or designee in each state agency that has custody, possession or control of employee information.
 - c. **Authorized Access.** The ability to examine CEI by an individual that has permission to view such information either by law, policy or written permission of the employee.
 - d. **Authorized Personnel.** An employee that has authorized access.

- e. **Confidential Employee Information (CEI).** Information pertaining to an employee that is held by the commonwealth in the role of an employer or in the role of a provider of employment-related services. Examples include, social security number and date of birth. Where federal or state law requires the protection of employee information, such information is CEI for the purposes of this directive.
- f. **Confidential Folder.** A secured file that is the official repository of confidential, investigative materials which may be stored either as a separate envelope in the Official Personnel Folder (OPF) or in the electronic OPF (e-OPF) in a separate secure electronic file location that is accessible only by authorized personnel.
- g. **Confidential Medical Folder.** A secured file that contains medical information related to absence requests, including sick, parental, family care, military caregiver, or Workers' Compensation absences, and records required to be maintained for medical monitoring of employees who are or have the potential to be exposed to hazardous materials.
- h. **Contractor.** Any person or organization that has entered into a contract with a commonwealth agency, department, board or commission.
- j. **Data Element Encryption.** Technique that protects individual data elements instead of encrypting an entire file or database.
- k. **Employee Information.** Information related to an employee's employment that is in the possession, custody or control of the Agency HR Records Custodian and/or the Office of Administration (OA) or State Records Center (SRC).
- l. **File Level Encryption.** Technique used that encrypts a file on a file system without encrypting the entire system or disk. This is used when files contain protected data transferred on physical media, email, or across networks without an already existing encryption protection.
- m. **Full Disk Encryption.** Technique used for devices with limited security controls.
- n. **Non-Public Employee Records.**
 - (1) The following employee information is generally not considered a "public record":
 - (a) Reference letters, unless prepared in relation to the appointment of an individual to fill a vacancy in an elected office or an appointed office requiring Senate confirmation.
 - (b) An Employee Performance Review or similar rating or review.
 - (c) The result of a civil service or similar test administered by a commonwealth, legislative or judicial agency.
 - (d) The result of a civil service or similar test administered by a local agency, if restricted by a collective bargaining agreement. Only test scores of individuals who obtained a passing score on a test administered by a local agency may be disclosed.
 - (e) The employment application of an individual not hired.
 - (f) Workplace Support Services Program information.
 - (g) Written criticism of an employee.

- (h) Grievance material, including records related to discrimination or sexual harassment.
 - (i) Written information regarding discipline, demotion or discharge of an employee contained in the OPF or other personnel file, other than information regarding the final action of an agency that results in demotion or discharge.
 - (j) Academic transcripts.
- (2) Information regarding individual gender may be provided in aggregate form, as such information is solely compiled under provisions of The Public Law 88-352, Title VII of the Civil Rights Act of 1964, as amended by the Equal Employment Opportunity Act of 1972 for reporting purposes and employees who provide this information are informed that this information is solely accumulated for that purpose; the information by individual may generally be exempt under Section 708(b)(2) and (6) of the RTKL, 65 P.S. § 67.708(b)(2) and (6).
- o. **Official Personnel Folder (OPF).** The hard copy or electronic (e-OPF) repository of employee information, which includes permanent employee information and temporary employee information that documents the employment work record.
 - p. **Permanent Employee Information.** Formal documentation of a person's current employment status and employment history.
 - q. **Programs.** Functions and services administered or managed by HR offices.
 - r. **Public Employee Information.** Public employee information pertaining to most commonwealth employees for the purpose of this directive consists of employing agency; last name; first name; organization name; job (class) code; job (class) name; headquarter agency address, headquarter agency telephone number; bargaining unit; biweekly salary; hourly rate; per diem rate; pay schedule; pay level; pay scale group; and years of service.
 - s. **Release.** Disclosure of confidential employee information.
 - t. **Retention.** The duration of time for which records must be kept in storage. This applies to both hard copy documents and electronic copies of documents.
 - u. **Storage.** The method and location in which records are retained.
 - v. **Temporary Employee Information.** Information which does not make a significant contribution to a person's employment record or which becomes outdated or inaccurate because of the passage of time.

5. POLICY.

- a. *Management Directive 205.36, Right-to-Know Law Compliance*, establishes policy and procedures for responding to requests for access to or copies of "public records" pursuant to the RTKL. In order to determine whether a document is subject to disclosure under the RTKL, the agency receiving a written request should conduct an initial review under procedures set forth in Section 7 of *Management Directive 205.36, Right-to-Know Law Compliance*.
- b. An employee may review or inspect his/her own employee information during regular work hours; in the case of an e-OPF, an employee may opt to do so outside of regular work hours. Any request by an employee to review or inspect their own employment files will be done in accordance with The Act of November 26, 1978, P.L. 1212, No. 286,43 P.S. § 1322.

- c. Personnel records are to be retained in accordance with *Manual 505.4, Personnel Records Retention and Disposition Schedule*.
- d. Policy and procedures regarding the management of commonwealth records are to be consistent with this directive and *Executive Order 1992-1, Records Management*, and *Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program*.
- e. Policy and procedures regarding the sending, accepting, storing or using of electronic records are to be consistent with this directive and with *Management Directive 210.12, Electronic Commerce Initiatives and Security*.
- f. Maintenance and release of employee information must be in compliance with applicable federal and state law and regulations (e.g. the Health Insurance Portability and Accountability Act (HIPAA) or RTKL).

g. Personnel Records.

- (1) All personnel records of active and inactive employees are the property of the commonwealth. The OPF and/or e-OPF are the official repository of personnel records. An OPF is to be established for each employee upon initial hire or retrieved from the SRC or former agency or field facility upon rehire and converted to an electronic format.
- (2) OPFs for active employees are to be maintained in agency headquarters HR offices unless they have been converted to an e-OPF. Exceptions to maintaining the OPF at agency headquarters are granted for the following agencies, which may designate their agency field locations as OPF retention sites:
 - (a) Department of Corrections.
 - (b) Department of Public Welfare.
 - (c) Department of Transportation.
 - (d) Department of Military and Veterans Affairs.
 - (e) Department of Conservation and Natural Resources.
- (3) The SRC is the official repository of all personnel records for inactive employees that do not have an e-OPF. Records for employees age 72 or older that do not have an e-OPF should be retained by the agency for four years after the date of separation and then destroyed.
- (4) Documents maintained in OPFs are classified as permanent or temporary employee information. Permanent employee information will, in all cases, remain in the OPF when an employee transfers or separates. Temporary employee information is to be retained for four years, unless otherwise required by policy or law, and then is to be purged in accordance with Section 7, Procedures.
- (5) The following employee information is specifically prohibited from being placed in OPFs:
 - (a) Arrest reports or criminal history records.

- (b) Investigative material regarding a civil, criminal, or administrative investigation of alleged wrong-doing by an employee where the charges were not sustained. However, when an employee requests in writing that such information be retained in order to support his or her defense of future allegations or charges that may be made, the agency may retain such material. Material related to ongoing investigations of matters regarding arrests/allegations is to be maintained in the confidential folder until the matter is resolved; the content is to be removed prior to review of the OPF by anyone who does not have a need to know the status of the investigation.
 - (c) National identification (other than IRS I-9 form).
 - (d) Birth certificates/baptismal certificates.
 - (e) Racial identification.
 - (f) Ethnic information.
 - (g) Political affiliation.
 - (h) Religious affiliation.
 - (i) Photo identification. (Maintain in separate file.)
 - (j) Written criticisms of which an employee is not aware.
 - (k) State Ethics Act and Code of Conduct financial disclosure forms and supplementary employment information. (Maintain in separate file.)
 - (l) Employee health and medical information including health enrollment forms, Workers Compensation records, medical information to support an absence, employer-based SEAP referral documents, disability related information, medical monitoring records, Right to Know hazardous chemical exposure records and any HIV/AIDS information as outlined in *Management Directive 505.26, HIV/AIDS and Other Bloodborne Infections/Diseases in the Workplace*. (Maintain in confidential medical folder and release only on a need to know basis with proper authorization and consistent with HIPAA and other relevant guidelines.)
 - (m) Grievance materials, including documents related to discrimination or sexual harassment, are to be maintained in a separate file. Exceptions include grievance settlements related to absence or pay adjustments and modification of personnel actions.
 - (n) Separate secure subject files containing employee information that are prohibited from being placed in OPFs are to be maintained consistent with the policies applicable to the relevant subject matter.
- (6) Documents related to the following subjects are prohibited from being in the OPF and should be maintained in a separate folder. This list may not be all inclusive.
- (a) State Ethics Act and Governor's Code of Conduct Statements of Financial Interest forms.
 - (b) Supplementary employment information.
 - (c) Sick, Parental and Family Care Leave medical documentation.
 - (d) Workers' Compensation claim forms and supporting documentation.

- (e) Disability related requests and supporting documentation.
- (f) Right to Know Health/Medical Exposure File.
- (7) If any procedure in this directive conflicts with any provision in a collective bargaining agreement, which provision is otherwise lawful, the provision of the collective bargaining agreement is controlling.
- (8) Employees have a right to submit rebuttals to any material in their OPFs. Rebuttals are to be acknowledged by Agency HR Records Custodians. Rebuttals and acknowledgements become part of the OPF in the same permanent or temporary category as the material being rebutted. If rebuttals are submitted by inactive employees, the most recent employing agency will acknowledge the rebuttal and send both the rebuttal and the acknowledgement to the SRC for inclusion in the inactive employee's OPF or convert to an electronic format for inclusion in the e-OPF.
- (9) For employees exposed to hazardous chemicals, a separate "Right to Know Health/Medical Exposure File" must be established and maintained consistent with the requirements of the Worker and Community Right-to-Know Act, 35 P.S. § 7301 et seq. and *Management Directive 505.27, The Worker and Community Right to Know Act (Chemical Right to Know)*. The employee's OPF must be annotated to show that this separate file exists.

h. Type of Information Maintained. The following types of employee information are permanent employee information and must be included in the OPF. This is not an all-inclusive list of information appropriate for maintenance in OPFs. Questions regarding the appropriateness of maintaining other data should be referred to OA, Office for Human Resources Management.

- (1) Most recent agency employment application/resume provided by the employee.
- (2) Agency notifications to employees regarding appointment, promotion, demotion, involuntary retirement, resignation by reason of abandonment of position, furlough, reassignment, transfer, salary changes (except general pay increases and longevity increments), dismissal, suspension, change in Civil Service status, and temporary assignment in a higher classification.
- (3) Extraordinary leave records, such as adjustments to leave service credits, requests and approval/disapproval notification for special extension of sick leave, and leaves of absence of longer than one full pay period.
- (4) Employee-initiated acknowledgements of temporary employment or unusual conditions of employment, such as the certificate required for employment of minors.
- (5) Employee requests and agency responses concerning voluntary retirement, voluntary separation, transfer, and demotion.
- (6) Any form of official recognition given to an employee that relates to his or her duties and responsibilities with the commonwealth.
- (7) Pre-employment background reports developed by the State Police, State Civil Service Commission, Office of Attorney General, and other agencies that are used to determine an employee's suitability for employment. In addition, agency background reference checks for employees required by their job duties to have Commercial Driver's License (CDL) are to be maintained. Pre-employment background reports and background reference checks should be maintained in a confidential folder within the OPF and removed prior to review of the OPF by the employee/representative.

- (8) Investigative reports prepared as a result of alleged wrongdoing by an employee should be kept in a confidential folder in accordance with Section 5, paragraph g.(5)(b). If the accusations are not sustained, reports are to be purged immediately.
 - (9) Department of Defense Forms DD 214 when used for commonwealth employment purposes.
 - (10) Agency and commonwealth sign-off forms attesting to the employee's receipt of information, including, for example, agency orientation checklist, CDL employee and supervisory training acknowledgement forms, employee handbooks/manuals, Workers' Compensation Rights and Duties Acknowledgement form, and Internet/Email user agreement. In accordance with *Management Directive 210.12, Electronic Commerce Initiatives and Security*, agencies may choose to use an electronic record of receipt (i.e., storing employee acknowledgements of the Internet/Email user agreements). These electronic acknowledgements utilize the User ID/Password as a verifiable electronic signature. Electronic versions of this record must be held in a database and be retrievable upon management's request.
 - (11) Current annual CDL accident and motor vehicle violation check forms.
 - (12) Immigration and Naturalization Form I-9.
 - (13) Permanent restrictions regarding use of weapons.
- i. The following types of employee information are temporary employee information and are to be purged from the OPF in accordance with Section 7b. and *Manual 505.4, Personnel Records Retention and Disposition Schedule*:
 - (1) Written reprimand, written record of an oral reprimand, written record of counseling session, or temporary restrictions.
 - (2) Employee Performance Reviews completed more than three years ago.
 - (3) Record of professional affiliations.
 - (4) Outdated forms superseded by current information.
 - j. The following employee information is to be maintained separately from the OPF: Attendance records, which are to be extracted directly from SAP; and supervisors' or managers' notes and records on matters such as discipline or performance on specific work assignments. The former items should be maintained in accordance with the timeframes designated by *Manual 505.4, Personnel Records Retention and Disposition Schedule*. The latter items should be maintained separately from the OPF by supervisors/managers but may be subject to access by employees if they are used to support discipline and may be shared with replacement supervisors/managers. In instances where documents originating from an employee's supervisory file are utilized to effect disciplinary action against an employee, the employee and/or union is entitled, upon issuance of such discipline, to review and be provided with copies of such documents upon request.
 - k. If a personnel action is revised, only information concerning the revised action is to be maintained. Record of the original personnel action or records of any rescinded personnel actions are to be immediately removed from an employee's OPF.

I. Access, Storage, and Release of Employee Information.

(1) **Access.** All employee records containing CEI, whether in paper or electronic format, may be accessed and used only by authorized employees, whose authorized access shall be limited to the minimum information necessary to fulfill the functions of their positions.

(a) **Authorized Commonwealth Employees.** Employees that need to access CEI as part of their job duties.

1 A minimum necessary number of authorized employees should have keys or other means of access to drawers, cabinets, or rooms where CEI is stored.

2 CEI should not be removed from the worksite unless necessary for authorized employees to perform their job duties.

3 When CEI is in use, it must be kept inaccessible to and out of sight of unauthorized employees.

4 Access to CEI and medical information is granted on a need to know basis and in accordance with appropriate governing laws and commonwealth policies affecting those documents. All requests for access are to be made to the Agency HR Records Custodian or designee. The following are to have access to the OPF and CEI when needed in the performance of their duties:

a Governor and Lieutenant Governor (for all employees).

b Agency Equal Employment Opportunity staff.

c An employee's immediate supervisor and those in direct chain of command above the immediate supervisor.

d Staff of OA, Office for Human Resources Management.

e Staff of the Office of Inspector General.

f Designated staff of the SCSC.

g Staff or members of agency HR Management Consulting teams.

h Staff of investigative agencies when specific procedures and requirements have been satisfied as provided in Section 7, paragraph a.(1)

(b) **Contractors.** When contractors have responsibility for a function that requires access to CEI, the nature of that access, the confidentiality requirements, and the use for which the access is granted must be defined in the contract with the commonwealth.

- (c) **Employees.** An employee and persons with written permission of an employee are permitted upon request of the employee to review that employee's OPF. Such reviews must be conducted in the presence of the Agency HR Records Custodian or designee at times amenable to both, and an employee may have a union or other representative present. Employees may request copies of OPF documents but are not allowed to alter, remove, add, or replace any documents from the OPF without permission from the Agency HR Records Custodian. Agency HR Records Custodians may charge reasonable fees consistent with fees referenced in *Management Directive 205.36, Right-to-Know Law Compliance* when requested to provide copies of all materials contained in the OPF or when frequent requests for copies of materials are received from the same employee. Employees having access to designated parts of their OPF will be provided access instructions and procedures for completing or modifying applicable forms and printing documents for personal use.
- (2) **Storage.** Administrative, technical and physical protections and safeguards are to be in place to secure the storage of CEI.
 - (a) **Storage of Files.** e-OPFs will be stored in accordance with *Management Directive 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy* and separately from program files. Program files that do not contain CEI and need to be accessed by employees who are not Authorized Personnel must be kept separately from files that contain CEI. Program files containing CEI must be kept separately from the OPF and protected within a locked cabinet. Duplicate copies of CEI should not be kept.
 - (b) **Field HR Offices.** Agency field HR offices referenced in section 5.g.(2) may maintain OPFs at that facility and must fully comply with the guidelines of this policy to ensure the security, privacy and integrity of CEI.
 - (c) **Electronic Protection.** Full Disk Encryption is to be used on data stored on devices such as computers, laptop computers, or electronic mobile devices in public or unsecure areas. The media upon which the files are stored (i.e., flash drive, external hard-drive, CD) must also be locked in a secured area.
- (3) **Retention.** Program files containing CEI will be kept for no more than 7 years, except as otherwise directed in *Manual 505.4, Personnel Records Retention and Disposition Schedule* or *Manual 210.9, The Commonwealth of Pennsylvania General Records Retention and Disposition Schedule*.

6. RESPONSIBILITIES.

- a. **OA, Deputy Secretary for Human Resources Management,** as required by *Management Directive 505.7, Personnel Rules*, shall maintain a record of all employees and positions and develop adequate standards for the establishment and maintenance of employee records. This requirement is separate and distinct from those records maintained by SCSC for civil service employees pursuant to Section 206(4) of the Civil Service Act, 71 P.S. § 741.206(4).
- b. **Agency Heads** shall ensure that necessary procedures and safeguards are implemented in accordance with this directive.
- c. **HR Directors** shall:
 - (1) Assign authorized personnel to have access to CEI.

- (2) Implement protections that limit the access to CEI to those who have a legitimate work-related need to access the information. Administrative, technical, and physical protections must be in place for all CEI at all times. Such methods of protecting that information include, but are not limited to, a locked drawer or room and data encryption. Drawers or rooms must be locked during non-business hours or whenever Authorized Personnel are not present. CEI sent to a printer or fax machine within an open area must have protections in place in order to keep that information private, such as a security code required on delayed print option or a coversheet used to protect the contents of the document from the casual passing viewer.

d. Supervisors shall:

- (1) Be responsible for approving and monitoring specific CEI released from supervisory files to Authorized Personnel, as well as maintaining and protecting supervisory files within the workspace.
- (2) Specify, in conjunction with HR Directors or their designees, per 6.c. of this directive, which positions may have access to CEI by assigning the role and responsibilities of the role and include in the employee's position description.

e. Authorized Personnel shall:

- (1) Use CEI to perform job duties and shall not disclose CEI to anyone other than as authorized.
- (2) Secure and Protect CEI within their workspace.
- (3) Safeguard, disclose, withhold, and dispose of information in accordance with this directive and ensure that information under their control is not accessible to unauthorized persons or used for non work-related purposes.

f. OA shall manage the electronic information systems and establish policy and procedures for the electronic maintenance and release of employee information.

g. SRC shall store and control hard-copy OPFs of inactive employees until the year of the individual's 75th birthday. At that time, the OPFs are to be destroyed. In addition, the SRC shall provide employee information to agencies, inactive employees, and other authorized personnel, as prescribed in this directive.

h. OA, Office for Human Resources Management shall audit the implementation of this directive and review complaints and appeals concerning delays in the provision of or denials of access to employee information.

7. PROCEDURES.

a. REQUEST FOR INFORMATION. Requests for non-public employee records are to be handled as follows:

- (1) An employee's home address may be furnished to law enforcement or court officials upon agency receipt of a written request showing that an indictment has been returned against an employee or a complaint, information, accusation, or other writ has been filed against an employee and the home address is needed to serve a summons, warrant, or subpoena. The home address may also be provided to authorized employees in case of emergencies.

- (2) An automated verification service that allows employees to have their employment and salary verified is available through TALX Corporation. The Work Number of Everyone, Customer Service Center (1-800-996-7566 or www.theworknumber.com) is available to answer questions from both employees and lenders/verifiers for such activities as mortgage applications, reference checks, loan applications, apartment leases or anything that requires proof of employment. Requests for employment salary verification are to be referred to this number. Specific procedures for accessing the system also can be obtained from agency HR offices.
- (3) An employee's social security number and home address may be furnished to taxing authorities upon written request.
- (4) Employee medical information may be furnished consistent with HIPAA and other relevant guidelines for release of personal information:
 - (a) when it is needed to aid medical treatment and an employee is not able to provide the information; or
 - (b) to a federal or state investigative agency when requested information is required to verify adherence to regulations. Employees need not be notified of the release of this information to federal or state investigators who must periodically verify the receipt of physical examinations by direct care employees; or
 - (c) when it is needed for another matter, such as Workers' Compensation proceedings.
 - (d) if enrollment information is requested, it should be referred to the HR Service Center.
- (5) Any information available to an employee from his or her own OPF may be released upon written authorization of the employee.
- (6) An agency's Office of Chief Counsel shall be notified immediately when any agency receives a subpoena or other written judicial order for employee information. The agency's Office of Chief Counsel shall make a determination as to the response to a subpoena or judicial order. The commonwealth should comply with a subpoena which appears on its face to be: lawfully issued; relevant to the legal proceeding; and not overly broad in scope, provided there is no compelling policy or legal reason to the contrary. Before complying with the subpoena, the Agency HR Records Custodian or designated authority shall take all reasonable steps to advise an employee whose records are being subpoenaed that a subpoena has been served, that the commonwealth may comply with the subpoena, and provide the employee with five days to consult with a private attorney to seek to have the subpoena quashed. Should the Agency HR Records Custodian be otherwise unable to contact the employee, the Agency HR Records Custodian will, by certified mail, return receipt requested, mail notification of the subpoena to the employee's last known address. The Agency HR Records Custodian shall also notify OA, Office of Chief Counsel of the receipt of the subpoena or other written judicial order for employee information and confirm that the above-mentioned steps have been taken.
- (7) Requests for information contained in pre-employment background investigations from employees or persons with written authorization are to be handled as follows:
 - (a) Requests are to be sent to the OA, Deputy Secretary for Human Resources Management.

- (b) OA, in conjunction with agency staff and the Office of General Counsel will develop appropriate responses and summaries of information contained in the reports.
 - (c) A permanent record of the release of this information, showing to whom it was provided and the date of release, is to be maintained in an employee's OPF and sent to the employee.
- (8)** Non-public employee information may be released to state investigative personnel when needed in the performance of their official duties. Proper identification must be provided and requesters must state specifically what information is needed. The following agencies are to be provided non-public information upon request in accordance with this paragraph. (Note: The following list is not all-inclusive and may include other investigative agencies with subpoena authority.)
- (a) Pennsylvania Human Relations Commission.
 - (b) Auditor General.
 - (c) Office of General Counsel.
 - (d) Pennsylvania State Police.
 - (e) Capitol Police.
 - (f) Office of Attorney General.
 - (g) Office of Inspector General.
 - (h) State Ethics Commission.
 - (i) Parent Locator Service, Department of Public Welfare.
 - (j) OA/Agency HR Management Consulting teams.
 - (k) Federal law enforcement, local police, and investigative agencies are to be provided, upon request, employee information deemed a public record. Requests from these agencies for non-public employee record are to be honored only if the requested information is determined to be relevant to the investigation or audit and is within the statutory authority of the requesting agency. Entire OPFs are not to be released unless all information contained therein is relevant to the investigation or audit. Questions concerning the release of such information should be referred to the agency's Office of Chief Counsel. If it is determined that requested information is irrelevant or not in accordance with law, the requester is to be so informed and advised that the request can be referred to OA, Deputy Secretary for Human Resources Management or the requester can seek a subpoena.
 - (l) Replies to inquiries from prospective non-commonwealth agency employers concerning specific reasons for a former employee's separation from employment are to indicate only whether the separation was voluntary or involuntary. Particular circumstances or issues involved in an involuntary separation or discipline are not to be disclosed without prior, written authorization of the former employee or unless specifically authorized by OA, Office for Human Resources Management.

- (9) SRC and Agency HR Records Custodians are authorized to release pertinent employment information when an employee is being considered for employment/transfer, from one commonwealth agency to another, or within an agency, or when an employee is to be reemployed by the commonwealth. The following information, consistent with purging requirements outlined in Section 7b. of this directive, in addition to public employee information, is to be provided in these cases upon written request indicating the employee is being considered for employment/transfer:
- (a) Employee Performance Reviews.
 - (b) Records of discipline, such as letters of caution, reprimand, admonishment, warning, or temporary restrictions.
 - (c) Letters of suspension and dismissal.
 - (d) Letters of commendation.
 - (e) Records of absence.
 - (f) Training records.
 - (g) Employment history data (consists of the above data on file from each agency in which the employee was employed by the commonwealth).

NOTE: The Agency HR Records Custodian is to notify an employee of what information has been referred to the requestor. If an individual is not subsequently accepted for transfer or reemployment, all information is to be returned to the forwarding agency/SRC. Use of this information for any other purpose is strictly prohibited.

- (10) Requests from union officials for employee information are to be honored when the information requested is relevant and necessary to the union's responsibilities in representing the bargaining/supervisory unit, consistent with the provisions of the *Public Employee Relations Act, Act of July 23, 1970, P.L. 563, No. 195, as amended (43 P.S. §§ 1101.101 - 1101.2301)*, and applicable collective bargaining agreements/memoranda of understanding. If a union request seeks information that is CEI or may otherwise be subject to protection from disclosure, consultation with labor relations and/or legal staff should occur. Information is to be provided within a reasonable period of time. Unless excessive costs are involved in compiling/mailling the information, the information should be provided without charge.
- (11) Any requests for the compilation of public employee information are to be addressed in accordance with *Management Directive 205.36, Right-to-Know Law Compliance*.
- (12) Requests for public employee information from state legislators and their staff are to be referred to the Legislative Data Processing Center at 717.787.7358.
- (13) Requests to review OPFs by employees located at facilities other than at the location where the OPFs are maintained are to be responded to as follows:
- (a) Employees are to be advised that they may choose to travel to the location where the OPF is maintained. Travel expenses and administrative leave will not be authorized for this purpose.

- (b) Upon request, the contents of an employee's OPF are to be duplicated and forwarded for review generally without cost to the employee. Employees may be charged reasonable fees for the cost of reproducing and mailing material in their OPF if such requests become excessive.
 - (c) The custodian will attach to the OPF a signed statement certifying that the entire contents of the folder were copied and are contained in the folder sent to the employee.
 - (d) Employees will have access to the e-OPF through Employee Self Service (ESS).
- (14) In the event of unauthorized release of non-public employee information, the agency HR Director must report the disclosure to the agency's Office of Chief Counsel. The agency's Office of Chief Counsel will work with the Office of General Counsel to respond accordingly.

b. REVIEW/PURGE OF OPFs.

- (1) OPFs shall be reviewed and purged according to the records retention schedule. Employees should be notified prior to the information being purged from the e-OPF.
- (2) HR Offices should ensure date-sensitive information is removed in a timely manner.
- (3) If the employee does not request the purged information, it should be shredded or disposed of confidentially.
- (4) Agency labor relations offices shall be notified prior to the removal of letters of caution, reprimand, admonishment, or warning. These letters are to be purged after two years if no similar incidents have occurred, unless:
 - (a) the letter constitutes a basis upon which a subsequent, i.e., progressive level of discipline was imposed; or
 - (b) there is a grievance pending over the letter or over a subsequent discipline for which the letter served as a basis. In such situations, the letter should remain in the employee's OPF for two years from the date of the subsequent discipline or, if a grievance has been filed, until the grievance is resolved; or
 - (c) another officially agreed-upon removal date has been designated.

c. TRANSFER OF OPF'S.

- (1) Upon separation from commonwealth employment, OPFs will be converted to an electronic format and maintained indefinitely.
- (2) OPFs of transferring employees are to be provided to gaining agencies when such agencies are under the Governor's jurisdiction. This includes confidential folders that are maintained for the employee. It is the gaining agencies' responsibility to convert and maintain all applicable records in the OPF.
- (3) Dual Employment. If an employee has dual employment with another state agency and resigns from one agency, the OPF should be converted to an electronic format and maintained in SAP by the retaining agency. While the employee retains dual employment, both agencies should have record of the dual employment in the OPF.

d. ACCESS TO INACTIVE EMPLOYEE RECORDS.

- (1) The SRC will provide access to OPFs of inactive employee as follows:
- (a) Public employee information will be provided to the most recent employing agency within a reasonable period of time upon request pursuant to the provisions of this directive.
 - (b) Non-public employee information will be furnished upon request from the employee's most recent employing agency. Information will be provided to clearly identified former employees or persons with letters of authorization from former employees. Restrictions on release of investigative reports, as per Section 5.h.(8) apply.
 - (c) OPFs will be made available to commonwealth agencies upon:
 - 1 request by the agency indicating that the employee was previously employed by the requesting agency;
 - 2 request by the agency indicating the employee has been employed by the commonwealth and the OPF is needed for active employment use; or
 - 3 authorization from the most recent employing agency; or
 - 4 written authorization by the employee.
 - (d) Procedures for the maintenance and release of e-OPFs for transferred/separated employees will be provided as agencies receive authorization for such files.

This directive replaces, in its entirety, Management Directive 505.18, dated May 29, 2012.