

# ***GENERAL OPERATIONAL INFORMATION***

---

- 103.1 GENERAL POLICY & REGULATION**
- 103.2 DEFINITIONS & ACRONYMS**
- 103.3 GOALS & OBJECTIVES**
- 103.4 FUNDING**
- 103.5 SUBSIDIZED CHILD CARE PROGRAM OBJECTIVES**
- 103.6 CONTACT INFORMATION**
- 103.7 MISSION STATEMENT**
- 103.8 CCIS GRANT**
- 103.9 PUBLIC ACCESS**
- 103.10 NONDISCRIMINATION**
- 103.11 CONFIDENTIALITY**
- 103.12 HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT (HIPAA)**
- 103.13 LIMITED ENGLISH PROFICIENCY (LEP)**
- 103.14 ACCEPTABLE USE OF INFORMATION TECHNOLOGY (IT) RESOURCES**
  - 103.14.1 General Policy
  - 103.14.2 Internet Use
    - 103.14.2.1 Software
    - 103.14.2.2 Expectation of Privacy – Internet
    - 103.14.2.3 Access & Authorization – Internet
    - 103.14.2.4 Acceptable Use - Internet
  - 103.14.3 E-mail Use
    - 103.14.3.1 Expectation of Privacy – E-mail
    - 103.14.3.2 Access & Authorization – E-mail
    - 103.14.3.3 Message Retention
    - 103.14.3.4 Security Issues
    - 103.14.3.5 Acceptable Use – E-mail
    - 103.14.3.6 Encryption
  - 103.14.4 Unacceptable Use of IT Resources
  - 103.14.5 Data Cleansing & Disposal of IT Resources
  - 103.14.6 Desktop & Server Software Patches
    - 103.14.6.1 Unsupported Software
    - 103.14.6.2 Microsoft Patches
- 103.15 CIS PASSWORDS**

# **GENERAL OPERATIONAL INFORMATION**

---

## **103.16 DEPARTMENT E-MAIL ACCOUNTS**

- 103.16.1 Granting & Removing Access to Generic Account – Option 1 Sites
- 103.16.2 Granting & Removing Access to R&R Account– Option 1 Sites
- 103.16.3 Accessing Accounts – Option 2 Sites
- 103.16.4 Account Passwords – All Sites
  - 103.16.4.1 Creating Passwords
  - 103.16.4.2 Changing Passwords
  - 103.16.4.3 Lock-outs

## **103.17 POLITICAL ACTIVITY GUIDELINES**

## **103.18 MILEAGE REIMBURSEMENT**

## **103.19 ORDERING FORMS & PUBLICATIONS**

## **103.20 FAMILY FILE & SUBPOENAS**

## **103.21 RECORD RETENTION**

## **103.22 REPORTING CHILD ABUSE**

## **103.23 PROVIDER COMPLAINTS**

## **103.24 WORKING WITH OTHER AGENCIES**

- 103.24.1 PA Key
- 103.24.2 County Assistance Office (CAO)
- 103.24.3 Employment & Training (E&T) Contractors
- 103.24.4 Regional OCDEL Offices
- 103.24.5 Internal Revenue Service (IRS)
- 103.24.6 Office of the Inspector General (OIG)
- 103.24.7 Office of Children, Youth and Families (OCYF) & Sharing Information regarding Keystone STARS Placements

## **103.25 HELPLINE**

## **103.26 HELP DESK**

## **103.27 STAFFING, TRAINING NEEDS & COORDINATION**

## **103.28 OCDEL RESPONSIBILITIES**

## **103.29 CCIS RESPONSIBILITIES**

## **103.30 USING PELICAN CCW**

## **103.31 UPDATED INFORMATION & ADDITIONAL RESOURCES**

- 103.31.1 Announcements
- 103.31.2 Updates
- 103.31.3 Communiqués
- 103.31.4 Additional Resources

# ***GENERAL OPERATIONAL INFORMATION***

---

## **103.32 TRAINING GUIDE**

- 103.32.1 Goals
- 103.32.2 Objectives
- 103.32.3 Section Checkpoint Questions
  - 103.32.3.1 Questions – 103.5 –Subsidized Child Care Program Objectives
  - 103.32.3.2 Questions – 103.9 –Public Access
  - 103.32.3.3 Questions – 103.11 –Confidentiality
  - 103.32.3.4 Questions – 103.12 –HIPAA
  - 103.32.3.5 Questions – 103.13 –LEP
  - 103.32.3.6 Questions – 103.14 –Acceptable Use of IT Resources
  - 103.32.3.7 Questions – 103.14.2.2 –Expectation of Privacy – Internet
  - 103.32.3.8 Questions – 103.14.3.1 –Expectation of Privacy – E-mail
  - 103.32.3.9 Questions – 103.14.3.4 –Security Issues
  - 103.32.3.10 Questions – 103.14.3.6 –Encryption
  - 103.32.3.11 Questions – 103.14.4 –Unacceptable Use of IT Resources
  - 103.32.3.12 Questions – 103.14.5 –Data Cleansing & Disposal of IT Resources
  - 103.32.3.13 Questions – 103.14.6 – Desktop & Server Software Patches
  - 103.32.3.14 Questions – 103.15 –CIS Passwords
  - 103.32.3.15 Questions – 103.16 –Department E-mail Accounts
  - 103.32.3.16 Questions – 103.16.1 – Granting & Removing Access to Generic Account – Option 1 Sites
  - 103.32.3.17 Questions – 103.16.4 – Account Passwords – All Sites
  - 103.32.3.18 Questions – 103.16.4.1 – Creating Passwords
  - 103.32.3.19 Questions – 103.16.4.2 – Changing Passwords
  - 103.32.3.20 Questions – 103.16.4.1 – Lock-outs
  - 103.32.3.21 Questions – 103.20 – Family File & Subpoenas
  - 103.32.3.22 Questions – 103.21 – Record Retention
  - 103.32.3.23 Questions – 103.22 – Reporting Child Abuse
  - 103.32.3.24 Questions – 103.23 – Provider Complaints
  - 103.32.3.25 Questions – 103.24.1 – PA Key
  - 103.32.3.26 Questions – 103.24.3 – E&T Contractors
  - 103.32.3.27 Questions – 103.24.4 – Regional OCDEL Offices
  - 103.32.3.28 Questions – 103.24.5 – IRS
  - 103.32.3.29 Questions – 103.24.7 – Sharing Information regarding Keystone STARS Placements
  - 103.32.3.30 Questions – 103.25 – Helpline
  - 103.32.3.31 Questions – 103.26 – Help Desk
  - 103.32.3.32 Questions – 103.27 – Staffing, Training Needs & Coordination

# ***GENERAL OPERATIONAL INFORMATION***

---

## **103.32.4 Section Checkpoint Answers**

- 103.32.4.1 Answers – 103.5 –Subsidized Child Care Program Objectives
- 103.32.4.2 Answers – 103.9 –Public Access
- 103.32.4.3 Answers – 103.11 –Confidentiality
- 103.32.4.4 Answers – 103.12 –HIPAA
- 103.32.4.5 Answers – 103.13 –LEP
- 103.32.4.6 Answers – 103.14 –Acceptable Use of IT Resources
- 103.32.4.7 Answers – 103.14.2.2 –Expectation of Privacy – Internet
- 103.32.4.8 Answers – 103.14.3.1 –Expectation of Privacy – E-mail
- 103.32.4.9 Answers – 103.14.3.4 –Security Issues
- 103.32.4.10 Answers – 103.14.3.6 –Encryption
- 103.32.4.11 Answers – 103.14.4 –Unacceptable Use of IT Resources
- 103.32.4.12 Answers – 103.14.5 –Data Cleansing & Disposal of IT Resources
- 103.32.4.13 Answers – 103.14.6 – Desktop & Server Software Patches
- 103.32.4.14 Answers – 103.15 –CIS Passwords
- 103.32.4.15 Answers – 103.16 –Department E-mail Accounts
- 103.32.4.16 Answers – 103.16.1 – Granting & Removing Access to Generic Account – Option 1 Sites
- 103.32.4.17 Answers – 103.16.4 – Account Passwords – All Sites
- 103.32.4.18 Answers – 103.16.4.1 – Creating Passwords
- 103.32.4.19 Answers – 103.16.4.2 – Changing Passwords
- 103.32.4.20 Answers – 103.16.4.1 – Lock-outs
- 103.32.4.21 Answers – 103.20 – Family File & Subpoenas
- 103.32.4.22 Answers – 103.21 – Record Retention
- 103.32.4.23 Answers – 103.22 – Reporting Child Abuse
- 103.32.4.24 Answers – 103.23 – Provider Complaints
- 103.32.4.25 Answers – 103.24.1 – PA Key
- 103.32.4.26 Answers – 103.24.3 – E&T Contractors
- 103.32.4.27 Answers – 103.24.4 – Regional OCDEL Offices
- 103.32.4.28 Answers – 103.24.5 – IRS
- 103.32.4.29 Answers – 103.24.7 – Sharing Information regarding Keystone STARS Placements
- 103.32.4.30 Answers – 103.25 – Helpline
- 103.32.4.31 Answers – 103.26 – Help Desk
- 103.32.4.32 Answers – 103.27 – Staffing, Training Needs & Coordination

# ***GENERAL OPERATIONAL INFORMATION***

---

## **103.1 GENERAL POLICY & REGULATION**

The purpose of the Subsidized Child Care Program is to provide financial assistance to pay for child care so that the parent/caretaker (p/c) can work, meet the County Assistance Office (CAO) Employment and Training (E&T) requirements, complete high school or participate in training while working a minimum of ten hours per week. **As set forth in § 3041.1 (relating to purpose), “The subsidized child care program is a nonentitlement child care program that is made available through limited Federal and State funds”.** The subsidized child care program is intended for families who meet the financial and nonfinancial eligibility criteria.

The subsidized child care program is available for families currently receiving Temporary Assistance for Needy Families (TANF), Food Stamps (FS)/Supplemental Nutrition Assistance Program (SNAP) benefits, families who received TANF benefits within the past 183 days (Former TANF or FT) and families of low-income (LI), including families who currently have children enrolled in Head Start (HS).

The subsidized child care program is administered by the Child Care Information Services (CCIS) agencies through Pennsylvania’s Enterprise to Link Information for Children Across Networks (PELICAN) Child Care Works (CCW). Within PELICAN CCW, there are six child care programs under which eligibility criteria are run to determine program eligibility or eligibility for enrollment (enrollment rules) for subsidy. The following are the child care programs that exist in PELICAN CCW:

1. TANF
2. FS/SNAP
3. FT
4. LI
5. HS

The Office of Child Development and Early Learning (OCDEL), Bureau of Subsidized Child Care Services manages the subsidized child care program for the Department of Public Welfare (Department). The Department implements the subsidized child care program through grants.

[Return to Table of Contents](#)

## **103.2 DEFINITIONS AND ACRONYMS**

See manual section **“101 – Definitions and Acronyms”** for a complete, alphabetical listing of definitions and an alphabetical table of acronyms.

[Return to Table of Contents](#)

## **103.3 GOALS & OBJECTIVES**

See Manual Section **“103.32.1 – Goals”** and Manual Section **“103.32.2 – Objectives”**

[Return to Table of Contents](#)

# ***GENERAL OPERATIONAL INFORMATION***

---

## **103.4 FUNDING**

State and federal funds are used to support the subsidized child care program.

Federal funding for subsidized child care is accessed by the Department as a benefit under Title XX of the Social Security Act and through the Child Care and Development Block Grant (CCDBG). OCDEL is responsible for the management of these federal funds for child care.

The goal of the Subsidized Child Care Program is to fully integrate all child care subsidies to provide a seamless funding system to qualified families needing subsidized child care.

[Return to Table of Contents](#)

## **103.5 SUBSIDIZED CHILD CARE PROGRAM OBJECTIVES**

The Department's overall objectives for the subsidized child care program are to:

1. Assist in the payment of child care services for eligible families whose children need child care while the p/c is working or meeting the CAO E&T requirements, completing high school or participating in training while working a minimum of ten hours per week.
2. Provide parent education regarding the benefits of quality child care.
3. Provide Resource & Referral (R&R) services free of charge to all families whether or not they qualify for subsidized child care.
4. Assure that an eligible family is able to choose a child care setting that is appropriate for the child(ren) in the family including licensed, registered and Relative/Neighbor (R/N) child care providers.
5. Allow a legally-operating child care provider the opportunity to participate in the subsidized child care program.
6. Distribute funds in a manner that maximizes the service funding available for subsidized child care.

[Return to Table of Contents](#)

[See Manual Section "103.32.3.1 – Questions – 103.5 – Subsidized Child Care Program Objectives"](#)

# ***GENERAL OPERATIONAL INFORMATION***

---

## **103.6 CONTACT INFORMATION**

See “[Contact Lists](#)” on OCDEL’s intranet site for information regarding the following:

1. CAO addresses for mailing.
2. CAO/CCIS contact persons.
3. CCIS agency information (i.e., CCIS Name, Address, Telephone Number, Facsimile Number, Primary Contact, Grantee, etc.).
4. Community Action Agency Contacts.
5. Pennsylvania Pre-K Counts (PKC) Grantees Contact List.
6. Regional Child Development Offices and Map.
7. Regional Key Contacts and Map.
8. Subsidy Coordinators.
9. Workforce Investment Area Contacts.
10. Commonwealth Directory.
11. OIG Regional Contacts.

[Return to Table of Contents](#)

## **103.7 MISSION STATEMENT**

The Department developed a Mission Statement for the CCIS. The Mission Statement sets forth the Department’s expectations for the manner in which subsidized child care services are provided to the community and speaks to the desired goal of customer service. The Mission Statement reads as follows:

“The Pennsylvania Department of Public Welfare through its CCIS agencies administers the subsidized child care program for low-income families and makes resource and referral services available to all citizens of Pennsylvania. CCIS agencies are dedicated to provide all services courteously, to help families receive all of the services for which they are eligible and to help families access all needed resources in a community.”

[Return to Table of Contents](#)

# GENERAL OPERATIONAL INFORMATION

## 103.8 CCIS GRANT

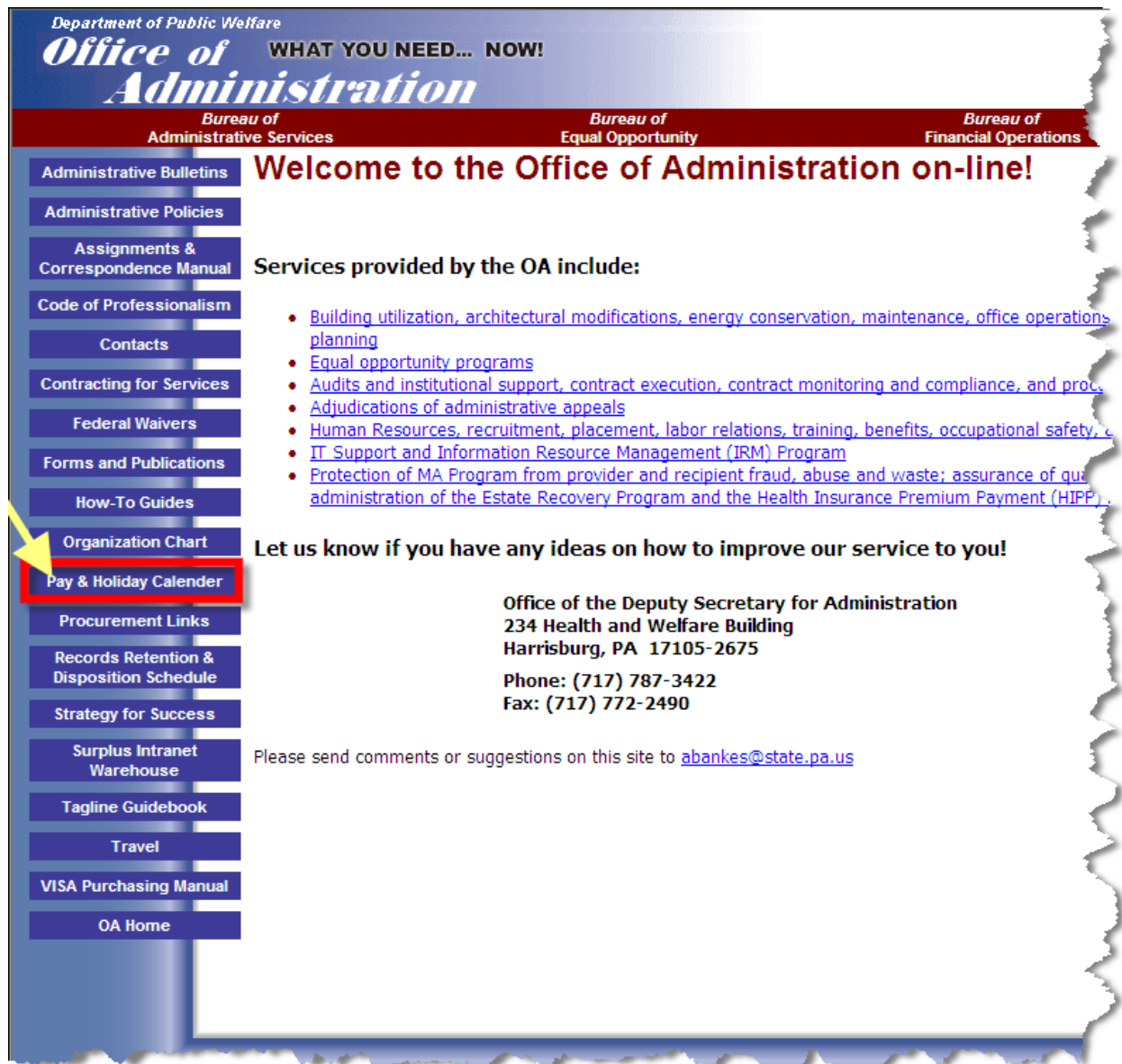
The CCIS must comply with the grant as set forth in [Section “100 – Grants & Subcontracting”](#).

[Return to Table of Contents](#)

## 103.9 PUBLIC ACCESS

The CCIS must be open for business and physically present to answer subsidized child care questions from the general public between the hours of 8:30 a.m. and 5:00 p.m., Monday through Friday, except on state-recognized holidays or in the case of County Government managed programs, county-recognized holidays.

A calendar listing the approved State holidays can be found at <http://oa/home/oahome.asp?hdrvalue=OA%20Home> by accessing the “Pay & Holiday Calendar” tab on the left navigation bar.



The CCIS must also be accessible to a p/c and/or provider who cannot contact the agency during the weekday office hours.



# **GENERAL OPERATIONAL INFORMATION**

---

A telephone call to the CCIS shall be toll-free for any family who lives within the county or geographical area served by the CCIS.

The toll-free telephone line may not have voice-mail as the primary mechanism for handling incoming telephone calls between the hours of 8:30 a.m. and 5:00 p.m., Monday through Friday, except on state-recognized holidays or in the case of County Government managed programs, county recognized holidays.

The CCIS will ensure that each of its staff responds to voice-mail messages within 2 working days. The CCIS shall be known as the “Child Care Information Services of \_\_\_\_\_ County”. The CCIS shall list the above-mentioned name prominently at the office location and on all correspondence to parents, providers and the general public.

On regular workdays during regular work hours, the State regulations, bulletins, operations memoranda, procedures and any supplemental instructions used to determine eligibility for the subsidized child care program must be available for review.

In addition, all CCIS agencies must have available a copy of 55 Pa. Code, Chapters 168 (relating to child care) and 3041 (relating to subsidized child care eligibility).

For a map and contact information for the Regional OCDEL Offices, see “Regional Child Development Offices and Map” under “**Contact Lists**” on OCDEL’s intranet site.

The CCIS must have a grievance procedure that handles client, provider and public complaints and unresolved issues.

[Return to Table of Contents](#)

[See Manual Section “103.32.3.2 – Questions – 103.9 – Public Access”](#)

## **103.10 NONDISCRIMINATION**

As set forth in **§ 3041.11(a)** (relating to nondiscrimination), “The CCIS may not discriminate against applicants for or recipients of Federal or State funds on the basis of age, race, sex, color, religious creed, national or ethnic origin, ancestry, sexual preference or physical or mental disability.”

The CCIS shall offer child care subsidy within the provisions of applicable civil rights laws and regulations, including the following:

- (1) **The Pennsylvania Human Relations Act (43 P.S. §§ 951 – 963).**

NOTE: Additional information regarding the Pennsylvania Human Relations Act may be found at the following websites:

[http://www.portal.state.pa.us/portal/server.pt/community/law/legalresources/18980/pennsylvania\\_human\\_relations\\_act/725567](http://www.portal.state.pa.us/portal/server.pt/community/law/legalresources/18980/pennsylvania_human_relations_act/725567)

- (2) **[The Age Discrimination Act of 1975 \(45 U.S.C.A. §§ 6101 – 6107\).](#)**

# GENERAL OPERATIONAL INFORMATION

---

- (3) [Title VI of the Civil Rights Act of 1964 \(42 U.S.C.A. §§ 2000d – 2000d-4a\).](#)
- (4) [Title VII of the Civil Rights Act of 1964 \(42 U.S.C.A. §§ 2000e – 2000e-15\).](#)
- (5) [Section 504 of the Rehabilitation Act of 1973 \(29 U.S.C.A. § 794\).](#)
- (6) [The Americans with Disabilities Act of 1990 \(42 U.S.C.A. §§ 12101 – 12210\).](#)

The CCIS may not discriminate against any applicant for or recipient of subsidized child care or any child care provider in the following areas:

- Program administration.
- Program participation.
- Eligibility determinations and redeterminations.
- Enrollment in facilities.
- Conduct of fair hearings.

The CCIS will not discriminate against any licensed, registered or R/N child care provider or limit a provider's ability to care for children who are eligible for the subsidized child care program.

For more information about the CCIS's responsibilities with regard to nondiscrimination, see the CCIS grant, Rider 4, #22 – Nondiscrimination/Sexual Harassment Clause.

[\*\*Return to Table of Contents\*\*](#)

## **103.11 CONFIDENTIALITY**

**As set forth in § 3041.83(a) (relating to confidentiality), “The CCIS and its employees shall keep confidential the information in the family file and use that information only for purposes directly connected to the administration of their duties.”**

With regard to families who are receiving TANF and/or FS/SNAP benefits and the subsidized child care related to those benefits, [\*\*55 Pa.Code, Chapter 105, § 105.1\*\*](#) (relating to policy) sets forth the legal provisions relating to policy for safeguarding information for applicants and recipients of public assistance by restricting the use or disclosure of the information as required by sections 404, 425 and 505 of the Public Welfare Code (62 P. S. §§ 404, 425 and 505).

Information contained in the family file is restricted to individuals connected with the administration of the Subsidized Child Care Program. Any member of the family or authorized person acting on behalf of the family, ***including advocates or legal representatives***, may review the family file during the CCIS agency's regular operating hours. A person other than those identified above may be permitted to access a family file only with the p/c's written permission.

# GENERAL OPERATIONAL INFORMATION

---

As set forth in [§ 3041.83\(b\)](#), “Agents of the United States, the Commonwealth and the Department who are responsible for eligibility review, evaluation or audit functions shall have access to, and the right to the use and disclosure of, information on applicants or recipients of subsidized child care. This use and disclosure is confined to the agent’s responsibility to carry out review, evaluation or audit functions.”

“Disclosure of information beyond the scope of review, evaluation or audit functions performed by the agents requires the p/c’s informed and written consent”, as specified in [§ 3041.83\(c\)](#).

As set forth in [§ 3041.83\(d\)](#), “Information in the family file may be disclosed to the local CAO when necessary to ensure that funds are authorized appropriately.”

“The CCIS shall assure the confidentiality of an individual who files an appeal or complaint about a family’s receipt of subsidized child care for a child”, as set forth in [§ 3041.83\(e\)](#).

All case information is considered confidential. There are some circumstances, which require the CCIS to take additional steps to further safeguard information. When a case meets any of the following conditions the CCIS must keep case comments in the hard file only (i.e., not within PELICAN CCW) and the hard file must be kept separate from other case files in a location that is secured and is accessible only by the Director or a designee of the Director’s choice:

1. Includes a teen parent who is 13 years of age or younger.
2. Includes an employee of the CCIS.
3. Includes an individual who has disclosed circumstances, which include domestic or other violence.

PELICAN CCW allows the CCIS to designate a case as “Confidential.” The CCIS may not use the functionality ***for any case in PELICAN CCW*** unless directed by OCDEL. This functionality restricts access to a confidential case by removing the hyperlink to the case from search pages and from the CIS Case Summary page.

The CAO has the ability to mark cases as confidential using the “DV indicator” in CIS. OCDEL continues to work closely with OIM to resolve issues related to accessing TANF, FS/SNAP and GA/WS2 case information once the confidentiality indicator is set.

When a new confidential TANF or FS/SNAP case is pushed or pulled into PELICAN CCW, the case will appear in the CIS Inbox and the CCIS will receive an alert that the CIS case is marked confidential. Existing confidential cases in PELICAN CCW also receive updates.

Only the primary and secondary CCIS caseworkers, as well as the Supervisor and Director who are assigned to the 0005 caseload will have access to new confidential cases.

**REMINDER:** Having a Director or Supervisor *security role* within PELICAN CCW does NOT mean the Director or Supervisor has access to the 0005 caseload and any confidential cases in that caseload. The Director or Supervisor User ID must be entered into the respective fields of the individual caseloads to establish access to the cases.

# GENERAL OPERATIONAL INFORMATION

---

NOTE: Users who may have multiple PELICAN CCW User IDs should be especially mindful of the User ID entered for the caseloads.

If the CCIS reassigns the TANF or FS/SNAP case to another caseload, then only those individuals assigned to the new caseload will be able to view the case unless they have a special confidentiality security role. If a CCIS worker who is not assigned to the caseload and does not have the special security role attempts to access a case, a warning is displayed indicating the worker does not have access.

If an individual is participating in more than one case, PELICAN CCW propagates the confidential status of the case to all cases in which that individual participates. If the CCIS staff assigned to the case in which confidentiality was propagated does not have the special security role, the staff will be unable to access case information.

## EXAMPLES:

1. If a CAO office marks a FS/SNAP case in their office confidential and that FS/SNAP case had a shared individual with a LI case, PELICAN CCW automatically considers the LI case confidential.
2. In joint custody cases in two different CCIS offices, if the CCIS or CAO marks one of the cases confidential, the other case with the shared child will be marked confidential.

When PELICAN CCW propagates confidentiality, an alert is generated to the primary worker of the case indicating that the case was marked confidential. A similar alert generates if confidentiality is removed from the case. Secondary workers may only view these alerts through an alert search.

To assist in determining the case that was originally marked as confidential, PELICAN CCW classifies confidentiality into one of two types:

1. ***Specified Confidential*** - indicates the case that was originally marked as confidential by the CCIS or CAO user.
2. ***Implied Confidential*** - indicates that PELICAN CCW propagated confidentiality to the case because a shared individual was marked as "Specified Confidential" in another case.

PELICAN CCW provides the "Specified" or "Implied" confidential designation on the Case Confidentiality Summary page. The CCIS may access the confidentiality designation information for a case by selecting Confidentiality in the "Select..." drop-down menu.

To "turn on" or "turn off" confidentiality in PELICAN CCW and to view Confidential cases without having the CCIS users assigned to a caseload, special confidentiality security roles were created. The Confidentiality security roles are:

- ***Confidentiality Read-Only*** – CCIS and CAO users with this role will be able to view confidential cases in their office.
- ***Confidentiality Super User*** – OCDEL HQ users or Help Desk/Superusers with this role will be able to view all confidential cases across the entire system.

# GENERAL OPERATIONAL INFORMATION

- **Confidentiality Update** – CCIS users with this role will be able to mark/unmark cases as confidential.
- **Confidentiality Fiscal Override** – CCIS users with this role will be able to view/modify payment related information (only on enrollment and co-payment screens) for confidential cases in their office.

Regardless of whether a CCIS user has the correct credentials to access the case, the CCIS Office cannot use the Case Confidentiality Summary to “turn off” confidentiality that was indicated in CIS nor can it “turn off” Implied Confidential functionality. Updates to a case’s confidentiality status do not display on the CIS Case Summary page. Alerts provide this information.

PELICAN CCW also disguises an individual’s SSN, displaying only the last four digits on the majority of the pages to help assure confidentiality and prevent identity theft issues.

Case Members			
Name	DOB	Gender	SSN
		Male	***_**_
		Male	***_**_
		Female	***_**_
		Female	***_**_
		Male	***_**_

[Return to Table of Contents](#)

[See Manual Section “103.32.3.3 – Questions – 103.11 – Confidentiality”](#)

## 103.12 **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)**

The *Standards for Privacy of Individually Identifiable Health Information* (Privacy Rule) establishes a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services (HHS) issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The Privacy Rule standards address the use and disclosure of individuals’ protected health information (PHI) by organizations subject to the Privacy Rule — called “covered entities,” as well as standards for individuals’ privacy rights to understand and control how their health information is used.

A major goal of the Privacy Rule is to assure that individuals’ health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public’s health and well being.

The Department is a covered entity as defined by HIPAA and is required to comply with the HIPAA privacy requirements. Each CCIS is a business associate of the Department as defined by HIPAA and therefore is also required to comply with the HIPAA privacy requirements.

# GENERAL OPERATIONAL INFORMATION

---

The CCIS must provide each p/c a notice of privacy practices (i.e., **Privacy Notice**) regarding how the CCIS will handle health information provided by the p/c. The **Privacy Notice** must be given to the p/c at the initial face-to-face interview. The **Privacy Notice** must also be posted in the CCIS office.

The **Privacy Notice** includes a signature line for the p/c; however, the p/c is ***NOT*** required to sign the notice. If the p/c refuses to sign the notice, the CCIS must note the refusal on the notice and place that copy of the notice in the family file.

The **Privacy Notice** informs the p/c of the following:

1. How the CCIS uses health information provided by the p/c.
2. P/C rights related to health information.
3. CCIS responsibilities related to handling health information.
4. CCIS contact information for a p/c that has questions regarding privacy requirements.
5. CCIS contact information for a p/c who wishes to report a problem related to how the CCIS uses health information.

The CCIS must maintain effective safeguards to protect the confidentiality of PHI. This includes administrative policies regarding handling and protection of records, physical safeguards such as locked files and technological security to assure PHI confidentiality.

PHI is defined as “individually identifiable health information”, including demographic data, which relates to the:

- Individual’s past, present or future physical or mental health or condition.
- Provision of health care to the individual.
- Past, present, or future payment for the provision of health care to the individual.
- Identification of the individual or for which there is a reasonable basis to believe it can be used to identify the individual.

PHI includes many common identifiers (i.e., name, address, birth date, Social Security Number).

A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual’s protected health information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information, except either as the:

1. Privacy Rule permits or requires.
2. Individual who is the subject of the information (or the individual’s personal representative) authorizes in writing.

The CCIS must disclose PHI in only two situations:

1. To individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their PHI.
2. To HHS when it is undertaking a compliance investigation or review or enforcement action.

# GENERAL OPERATIONAL INFORMATION

---

The CCIS must report security incidents or breaches related to PHI, as set forth in [Rider 6 - HIPAA Compliance](#).

Rider 6 of the CCIS Grant relates to privacy and security of PHI as required by HIPPA. Rider 6, Section 4 (c), requires the CCIS to report any improper use or disclosure of PHI to OCDEL's Agreement Officer. Section 4 (d) requires the CCIS to report any security incidents, such as theft or lost records, to the Agreement Officer. The CCIS must report all incidents of improper use/disclosure or other security violations to the Agreement Officer ***within two days of discovery***.

[Return to Table of Contents](#)

[See Manual Section "103.32.3.4 - Questions - 103.12 - HIPAA"](#)

## 103.13 **LIMITED ENGLISH PROFICIENCY (LEP)**

Title VI of the Civil Rights Act of 1964 prohibits discrimination on the basis of race, color or national origin in any program or activity that receives federal funds either directly or indirectly, through a grant, contract or subcontract. In addition, Title VI requires that timely, quality language assistance be provided to persons with LEP in order to assure such individuals receive meaningful access to federally funded programs and services.

For more information on LEP, visit OCR's website at:

<http://www.dhhs.gov/ocr/civilrights/resources/specialtopics/lep/>.

The following are examples of practices that may violate Title VI:

- Providing services to persons with LEP that are more limited in scope or are lower in quality than those provided to other persons.
- Subjecting persons with LEP to unreasonable delays in the delivery of services.
- Limiting participation in a program or activity on the basis of English proficiency.
- Providing services to persons with LEP that are not as effective as those provided to those who are proficient in English.
- Failing to inform persons with LEP of the right to receive free interpreter services and/or requiring persons with LEP to provide their own interpreter.

The CCIS must make reasonable accommodations for the language requirements of persons with LEP. To accomplish this, the CCIS may contract with the LanguageLine or any other equivalent service provider, in order to assist in working with persons with LEP.



# ***GENERAL OPERATIONAL INFORMATION***

---

The responsibilities under Title VI of the Civil Rights Act of 1964 follow:

1. The CCIS must comply with Title VI of the Civil Rights Act of 1964, 42 U.S.C. §2000d, by taking action, as required, to assure that all persons with LEP have meaningful access to the services administered by the grantee. This includes providing, free of charge, notice of the availability of language services to persons with LEP, translating vital documents into regularly-encountered languages spoken by persons with LEP and providing oral translation services as needed.
2. The CCIS must record in the client's case file any need for language services and take such measures as are appropriate to assure oral translation and written translation in order for the client to have meaningful access to services administered by the contractor.
3. The CCIS must provide the Department with a written LEP Plan upon request for compliance with Title VI of the Civil Rights Act of 1964 as it pertains to persons with LEP. The written plan must include the following:
  - a. Assessing the need for LEP services in your area of service.
  - b. Identifying the resources developed for translation of verbal and written information.
  - c. Establishing a plan to train all of your staff regarding their responsibility to accommodate persons with LEP.
  - d. Establishing a method to monitor the implementation and effectiveness of the LEP plan for compliance with Title VI of the Civil Rights Act of 1964.

The plan addresses each requirement for compliance with Title VI of the Civil Rights Act of 1964 as it pertains to persons with LEP. The type of language assistance the CCIS provides to assure meaningful access will depend on a variety of factors, including CCIS size, the size of the eligible LEP population served, the total resources available to the CCIS, the frequency with which particular languages are encountered, and the frequency with which persons with LEP come into contact with the CCIS. The CCIS must keep a copy of the plan for its permanent files.

[Return to Table of Contents](#)

[See Manual Section "103.32.3.5 – Questions – 103.13 – LEP"](#)



# GENERAL OPERATIONAL INFORMATION

---

## 103.14 ACCEPTABLE USE OF INFORMATION TECHNOLOGY (IT) RESOURCES

“Authorized Users” are defined as Commonwealth of Pennsylvania employees, contractors, consultants, volunteers and any other Authorized User who utilizes or has access to IT Resources.

Commonwealth IT Resources include but are not limited to the following:

1. The Commonwealth’s computer systems, together with any electronic resource used for communications, which includes, but is not limited to laptops and individual desktop computers.
2. Wired or wireless telephones, cellular phones, pagers, beepers, personal data assistants and handheld devices (i.e., a Blackberry device, Palm devices, etc., and, further, includes use of the Internet, electronic mail (e-mail).
3. Instant messaging, texting, voice mail, facsimile, copiers, printers or other electronic messaging through Commonwealth facilities, equipment or networks.

The [IT Resources User Agreement](#) must be reviewed and/or completed as specified in [Management Directive 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy](#).

[Return to Table of Contents](#)

[See Manual Section “103.32.3.6 – Questions – 103.14 – Acceptable Use of IT Resources”](#)

### 103.14.1 General Policy

All “Authorized Users” that have access to Commonwealth IT Resources must comply with the following standards:

1. **Ownership of IT Resources.**

All data and records, including those pertaining to computer use, Internet use, e-mail communication, voicemail communication, and other electronic communication (whether sent, received, or stored), as well as the content of such communications, are presumed to be the sole and exclusive property of the Commonwealth.

2. **Authorized Users should have no expectation of privacy when using IT Resources.**

At its discretion, the Department may access, retrieve, trace, audit, monitor and review any files, data or records which are stored on or accessed through IT Resources, as well as, data or records related to IT Resource usage, including Internet records or e-mail communications, in order to determine compliance with the all management directives, personnel policy or applicable local, state or federal law. Files, data and records which are stored on IT Resources may be reviewed at any time and are routinely backed up and stored without the user’s knowledge.

# GENERAL OPERATIONAL INFORMATION

---

3. **Authorized Users may not access unauthorized data.**

Authorized Users may not access any data or programs contained on Commonwealth systems for which they do not have authorization or explicit consent. CCIS agencies should be particularly mindful of this when accessing information contained in CIS. Authorized Users may not use non-Commonwealth or non-approved storage devices or storage facilities without the approval of OCDEL.

4. **IT Resources are intended for business use and must never be used in a manner that violates other Commonwealth directives and policies.**

IT Resources are made available for Commonwealth business purposes. Any personal use which is inconsistent with Commonwealth policy is prohibited. Authorized Users may not use IT Resources to engage in personal, for-profit transactions or business, or to conduct any fundraising activity not specifically sponsored, endorsed, or approved by the Commonwealth. All use of IT Resources must conform with [Executive Order 1980-18, Code of Conduct, Management Directive 505.7, Personnel Rules](#), and Commonwealth policies on nondiscrimination and sexual harassment. Violations of these directives and policies through IT Resources will be treated in the same manner as other violations. Authorized Users may not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of IT Resources; deprive an Authorized User of access to an IT Resource; obtain extra IT Resources beyond those allocated; or circumvent computer security measures. Authorized Users may not access, create, store, transmit, post or view material that is generally considered to be inappropriate or personally offensive or which may be construed as discriminatory or harassing, including sexually suggestive, pornographic or obscene material.

5. **All Authorized Users must sign an agreement and each agency must maintain copies of the signed agreement in that agency.**

As a condition of granting access to the IT Resources, agencies must obtain an acknowledgement of receipt and understanding in the form of a signed user agreement: [IT Resources User Agreement](#). Agencies must obtain signed user agreements prior to granting access to IT Resources. Completed user agreements shall be maintained as part of the employee's Official Personnel Folder. Alternately, users may sign and agencies may store these agreements in an electronic format consistent with [Management Directive 210.12, Electronic Commerce Initiatives and Security](#), and [1TB-SEC006, Commonwealth of Pennsylvania Electronic Signature Policy](#). Signed agreements must be accessible to individuals who are authorized to view or use the documents.

# GENERAL OPERATIONAL INFORMATION

---

6. **Requests for electronic records should be treated in the same manner as paper records.**

Requests for records pertaining to IT Resources must be addressed consistent with all laws, directives or policies that would apply to the same information if maintained in a non-electronic format. Keep in mind that the Commonwealth is committed to operating a government that is transparent to its citizens – meaning that government information is often available to the public upon request. These requests should be referred to the subsidy coordinator.

7. **Software, including shareware or freeware.**

Authorized Users may not make unauthorized copies of copyrighted software. Authorized Users may not use non-standard shareware or freeware software without agency IT management approval unless it is on the agency's standard software list. Authorized Users may not engage in illegal activity in connection with their use of IT Resources, including, but not limited to downloading, installing or running security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, Authorized Users may not run password cracking programs, packet sniffers, port scanners or any other non-approved programs on IT Resources, unless they are specifically authorized to do so

8. **Passwords & Encryption.**

Authorized Users must use passwords and/or encryption in a manner that is consistent with Commonwealth policy. Authorized Users must keep passwords secure and must not share them with others. Authorized Users may only use encryption methods approved by the Commonwealth to encrypt information. Authorized Users may not rely on any business communications via the Internet being secure, private, or inaccessible, even where appropriate security applications are used (i.e., data encryption).

[Return to Table of Contents](#)

## 103.14.2 **Internet Use**

All security policies of the Commonwealth and its agencies, as well as policies of Internet Web sites being accessed, must be strictly adhered to by Authorized Users.

[Return to Table of Contents](#)

# ***GENERAL OPERATIONAL INFORMATION***

---

## **103.14.2.1 Software**

In connection with Authorized Users' use of and access to IT Resources:

1. All software used to access the Internet must be part of the agency's standard software suite or approved by the agency IT department. This software must incorporate all vendor provided security patches.
2. All files downloaded from the Internet must be scanned for viruses using the approved Commonwealth distributed software suite and current virus detection software.
3. All software used to access the Internet shall be configured to use an instance of the Commonwealth's standard Internet Access Control and Content Filtering solution.

[Return to Table of Contents](#)

## **103.14.2.2 Expectation of Privacy – Internet**

All user activity involving internet use is subject to tracking, blocking, logging, auditing, monitoring, accessing, retrieving and reviewing by the Department.

[Return to Table of Contents](#)

[See Manual Section “103.32.3.7 – Questions – 103.14.2.2 – Expectation of Privacy – Internet”](#)

## **103.14.2.3 Access & Authorization – Internet**

Agencies should authorize access to the Internet using Commonwealth computer resources through the utilization of a user ID/password system. Security violations can occur through unauthorized access, and all possible precautions should be taken to protect passwords.

[Return to Table of Contents](#)

# ***GENERAL OPERATIONAL INFORMATION***

---

## **103.14.2.4 Acceptable Use - Internet**

Accepted and encouraged use of the Internet for Authorized Users on IT Resources includes, but is not limited to, the following:

1. Access, research, exchange or posting of information that relates to the assigned job duties of an Authorized User for carrying out Commonwealth business.
2. Promotion of public awareness in regard to Commonwealth law, agency services and public policies.
3. Posting of agency information that has been authorized by appropriate management.

If the CCIS uses a local website for its agency, the CCIS must:

1. Identify Department links.
2. Test each link for integrity.
3. Identify and correct outdated links using the information found at <http://www.dpw.state.pa.us>.

[Return to Table of Contents](#)

## **103.14.3 E-mail Use**

All security policies of the Commonwealth and its agencies must be strictly adhered to by Authorized Users.

[Return to Table of Contents](#)

### **103.14.3.1 Expectation of Privacy - E-mail**

1. When sensitive material is sent electronically via e-mail, it is important to verify that all recipients are authorized to receive such information and to understand that e-mail is not fully secure and/or private, except where appropriate security applications are used (i.e., data encryption).
2. Users should understand that messages can be quickly and easily copied and may be forwarded inappropriately.
3. Where it is necessary to transmit Commonwealth proprietary or restricted information beyond the Commonwealth Connect e-mail network, the messages should be protected by encryption. Authorized Users should contact their agency Network Coordinator or IT Coordinator for assistance if encryption is needed.

# GENERAL OPERATIONAL INFORMATION

---

4. The agency head or designee should determine specific agency policy regarding business information which is determined to be too confidential or sensitive to be transmitted via e-mail.
5. All user activity and electronic communication, including the contents of such communication, including but not limited to, e-mail, voicemail, text messages and data, on IT Resources is subject to tracking, blocking, logging, auditing, monitoring, accessing, retrieving and reviewing.

[Return to Table of Contents](#)

[See Manual Section “103.32.3.8 - Questions - 103.14.3.1 - Expectation of Privacy - E-mail”](#)

## **103.14.3.2 Access & Authorization – E-mail**

1. Only Authorized Users may use IT Resources to send or view e-mail or access the Commonwealth’s e-mail systems.
2. Unauthorized persons may not use the network or Commonwealth equipment to originate e-mail messages or read e-mail messages directed to others.
3. Access to Commonwealth e-mail will only be granted to Commonwealth employees, contractors, consultants, volunteers, in their capacity as Authorized Users, if they agree to abide by all applicable rules of the system.
4. An Authorized User may not access the e-mail or account of another Authorized User unless granted permission to do so by the Authorized User. Unauthorized access of an Authorized User’s e-mail files is a breach of security and ethics and is prohibited.
5. In accordance with agency policy, Authorized Users should use password protection to limit access to e-mail files. Authorized Users must safeguard their passwords so that Unauthorized Users do not have access to their e-mail. Authorized Users are responsible for all messages transmitted and originating under their account.

[Return to Table of Contents](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.14.3.3 **Message Retention**

All messages, including e-mail, text messages, and voice messages, are subject to the appropriate records retention and disposition schedules and the provisions of [Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program](#).

[Return to Table of Contents](#)

## 103.14.3.4 **Security Issues**

E-mail and attachments to e-mail increasingly are reported to be sources of computer viruses. All Authorized Users should act in accordance with the latest IT Bulletins regarding containment methods for computer viruses.

The CCIS user must secure his/her desktop computer when stepping away from his/her desk, even for only a few moments. In order to secure the desktop, the CCIS user must press “Ctrl” and “Alt” and “Delete” on the keyboard, then select “Lock Computer”.

For the safety of the Commonwealth network, if a CCIS user’s username, password or e-mail account is compromised the following may occur:

1. The user’s Commonwealth network account may be closed.
2. The user may be assigned a new account and e-mail address.

If a user is assigned a new account and e-mail address, the following are likely consequences:

1. Messages sent to the previous e-mail address will be returned to the sender as undeliverable. For security purposes, it is not possible to forward items from a previous e-mail address.
2. The user will lose many of the customized features in his/her personal e-mail box.
3. The user’s chief information officer and Deputy Secretary for Administration may be notified.

[Return to Table of Contents](#)

[See Manual Section “103.32.3.9 – Questions – 103.14.3.4 – Security Issues”](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.14.3.5 Acceptable Use - E-mail

1. Every Authorized User who uses IT Resources is responsible for ensuring posted messages and other electronic communications are professional and businesslike.
2. Review each e-mail message before it is sent and make certain that addresses are correct and appropriate. Use spell check before sending.
3. Consider that each e-mail message sent, received, deleted, or stored has the potential to be retrieved, seen, and reviewed by audiences, including the general public, who were not the intended recipient of the message.
4. Ensure that content is appropriate and consistent with business communication; avoid sarcasm, exaggeration and speculation which could be misconstrued. Remember that intonation and inflection are lost in e-mail.
5. Be as clear and concise as possible; be sure to clearly fill in the subject field so that recipients of e-mail can easily identify different e-mail messages.
6. Authorized Users should receive authorization from their supervisor before wide scale "broadcasting" an e-mail bulletin to groups of employees.
7. The use of "reply to all" should be avoided unless it is appropriate to respond to all addressees.
8. Attachments to e-mail messages should not be overly large. Technical standards such as file size and backup procedures, are available on the OA/OIT Internet Web site at [http://www.oit.state.pa.us/portal/server.pt/community/information technology/402](http://www.oit.state.pa.us/portal/server.pt/community/information%20technology/402).

[Return to Table of Contents](#)

## 103.14.3.6 Encryption

Use of the Commonwealth's e-mail system affords a secure method to both Option 1 and Option 2 CCIS sites to send and receive e-mail. Commonwealth e-mail includes an encryption feature that enables senders to make secure any e-mails sent to recipients outside the Commonwealth system.



# GENERAL OPERATIONAL INFORMATION

---

Encryption of an e-mail message requires that the external recipient register with the Commonwealth in order to be able to open and read the message. The registration process is “one-time only” and is prompted the first time the external recipient receives an encrypted e-mail from the Commonwealth’s system.

Users of Commonwealth e-mail should not encrypt e-mail being sent to recipients with “@.pa.gov”. Additionally, they should not encrypt e-mails being sent to recipients outside the Commonwealth system unless it contains sensitive information. Sensitive information includes:

- ✓ Social Security numbers.
- ✓ Financial data.
- ✓ Personal health information.
- ✓ Legal documents.
- ✓ Personnel information.
- ✓ General personal information.

If a user decides that an e-mail must be encrypted, he or she can do so by one of the following methods:

1. **Clicking the “Send Secure” button:**

- If using pre-2007 versions of Microsoft Outlook, the user will see this button in the e-mail message window. Click the “Send Secure” button located at the top left corner under the tool bar to encrypt and send the e-mail.
- If using Outlook 2007, the user will need to click the “Add-Ins” tab from the tool bar to access the “Send Secure” button.

2. **Typing certain filters into the subject line of the e-mail:**

To encrypt an e-mail message, the user can type the words “ENCRYPT” or [SEND SECURE] in the subject line of the e-mail. Note that these words must be in the upper case and typed in the subject line exactly as written above. This is the method of encryption that must be used if sending an e-mail from Outlook Web Access.

# GENERAL OPERATIONAL INFORMATION

---

### 3. Selecting “Confidential” from the sensitivity settings in Outlook

Users may select the “confidential” setting to encrypt an e-mail. To do this, click “Options” in the e-mail message window. Under “Message Settings”, select “Confidential” then click “Close”.

See the desk guide titled [Commonwealth E-mail Encryption](#) for additional information. Users may also access a web-based training for e-mail encryption on the Commonwealth’s Learning Management System. To do this:

1. Go to <http://lms.state.pa.us>.
2. Enter your CWOPA user name and password at the Log In.
3. Under “My Courses” select “Enrolled Courses”.
4. Locate the course “E-mail Encryption for Commonwealth Employees”
5. Click the “Launch” button and follow the instructions to complete the training.

If the CCIS experiences technical issues with the encryption feature, or if they have external recipients who are having difficulty registering with the Commonwealth, contact OCDEL at [RA-ocdelwebadmin@pa.gov](mailto:RA-ocdelwebadmin@pa.gov).

[Return to Table of Contents](#)

[See Manual Section “103.32.3.10 – Questions – 103.14.3.6 – Encryption”](#)

## 103.14.4 Unacceptable Use of IT Resources

The following are examples of impermissible uses of IT Resources. This list is by way of example and is not intended to be exhaustive or exclusive. Authorized Users are prohibited from:

1. Accessing, creating, storing, transmitting, posting or viewing material that is generally considered to be inappropriate or personally offensive or which may be construed as harassing, including sexually suggestive, pornographic or obscene material.
2. Accessing, creating, storing, transmitting, posting or viewing material that expresses or promotes discriminatory attitudes toward race, gender, age, nationality, religion, or other groups including, but not limited to, protected groups identified in [Executive Order 2003-10, Equal Employment Opportunity](#).

## ***GENERAL OPERATIONAL INFORMATION***

---

3. Engaging in personal, for-profit transactions or business, or conducting any fundraising activity not specifically sponsored, endorsed, or approved by the Commonwealth.
4. Participating in Internet activities that inhibit an employee's job performance or present a negative image to the public, such as auctions, games, or any other activity that is prohibited by directive, policy or law.
5. Attempting to test or bypass the security ("hacking" or "cracking") of computing resources or to alter internal or external computer security systems.
6. Participating in or promoting computer sabotage through the intentional introduction of computer viruses, worms or other forms of malware, i.e. malicious software.
7. Promoting, soliciting or participating in any activities that are prohibited by local, state, or federal law or the Commonwealth rules of conduct.
8. Violating or infringing the rights of any other person.
9. Using any other Authorized User's password and/or equipment to conduct unacceptable activities on IT Resources.
10. Harassing or threatening activities including, but not limited to, the distribution or solicitation of defamatory, fraudulent, intimidating, abusive, or offensive material.
11. Transmitting or soliciting any proprietary material, such as copyrighted software, publications, audio or video files, as well as trademarks or service marks without the owner's permission.
12. Promoting or participating in any unethical behavior or activities that would bring discredit on the Commonwealth or its agencies.
13. Downloading and/or installing any unapproved software.
14. Transmitting or posting any messages that intentionally misrepresent the identity of the sender, hide the identity of the sender or alter a sender's message.
15. Sending or forwarding confidential or sensitive Commonwealth information through non-Commonwealth e-mail or webmail accounts. Examples of non-Commonwealth e-mail accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, Gmail and e-mail provided by other Internet Service Providers.
16. Sending, forwarding or storing confidential or sensitive Commonwealth information utilizing non-Commonwealth accredited mobile devices. Examples of mobile devices include, but are not limited to, Personal Data Assistants, Blackberry devices, two-way pagers and cellular telephones.

# GENERAL OPERATIONAL INFORMATION

---

17. Participating in any other Internet or e-mail use that is deemed inappropriate by the Commonwealth and/or its agencies and is communicated as such to Authorized Users.

[Return to Table of Contents](#)

[See Manual Section “103.32.3.11 – Questions – 103.14.4 – Unacceptable Use of IT Resources”](#)

## **103.14.5 Data Cleansing & Disposal of IT Resources**

Citizen and agency data are to be securely erased from state-owned and leased devices/media. Peripheral storage devices including but not limited to floppy diskettes, CD and DVD discs along with external storage devices such as USB drives, are not to be used by end users for storing Commonwealth data. An exception may be made for specific tasks only if the user is directed to do so by his or her agency’s IT staff or administrator. In such cases the external storage media used are to follow the same guidelines as hard drives for purging data or are to be physically destroyed once retired or decommissioned. This also includes archive media such as tape backup. Additional information may be obtained from the Bureau of Information Systems, as needed.

[Return to Table of Contents](#)

[See Manual Section “103.32.3.12 – Questions – 103.14.5 – Data Cleansing & Disposal of IT Resources”](#)

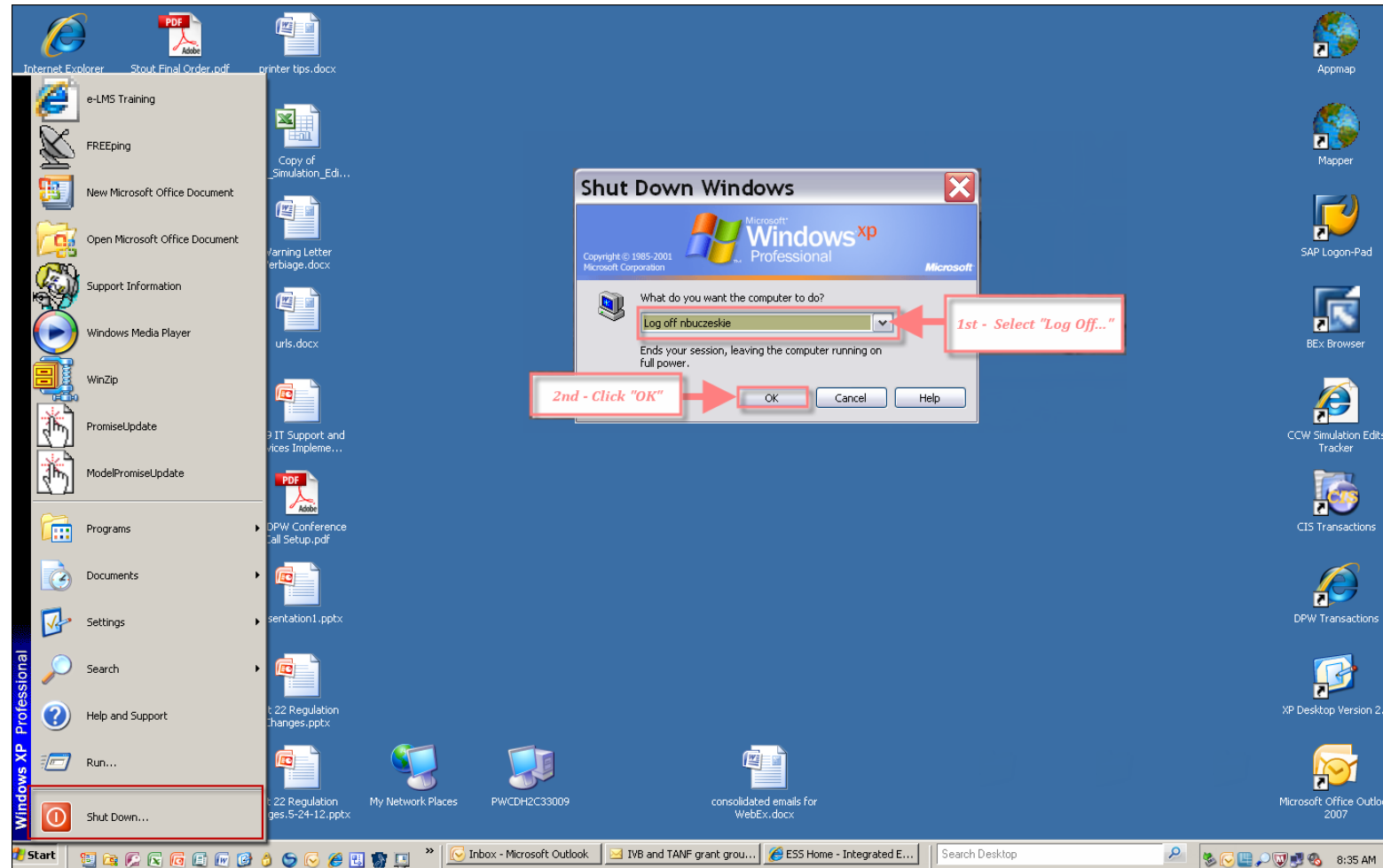
## **103.14.6 Desktop & Server Software Patches**

In an effort to better secure the Commonwealth network and computing infrastructure, all server and desktop platforms are to be kept up-to-date with service packs and security patches. Recent virus outbreaks have brought some agencies to a standstill, prevented access to the Internet, and in some cases caused loss of revenue to the Commonwealth from outages.

This policy covers ***ALL*** software in use on Commonwealth IT hardware assets, including operating systems, regardless of platform.

The CCIS must make sure all computers/tablets are logged off with power left on over the week-end in order to receive the security patches that will be sent out. To do this, the user must left click the “Start” button on the bottom left of the desktop, then clicks “Shut Down”. A dialog box will open prompting the user to indicate what the user wants the computer to do. The user must select “Log Off” and click “OK”.

# GENERAL OPERATIONAL INFORMATION



[Return to Table of Contents](#)

[See Manual Section "103.32.3.13 – Questions – 103.14.6 – Desktop & Server Software Patches"](#)

# ***GENERAL OPERATIONAL INFORMATION***

---

## **103.14.6.1 Unsupported Software**

In the Commonwealth, unsupported software is defined as software no longer supported by the vendor that produced it. Such software is not to be installed on Commonwealth production hardware.

[Return to Table of Contents](#)

## **103.14.6.2 Microsoft Patches**

Typically, Microsoft releases security patches on the second Tuesday of every month. CCIS agencies must leave computers on so the patches can be properly installed.

See the screenshot below for an example of how the security patch e-mail will appear to the user.

# GENERAL OPERATIONAL INFORMATION

## What is the purpose of this alert?

This is an advance notification of one out of band security bulletin that Microsoft intends to release on August 02, 2010.

The bulletin addresses a security vulnerability in all supported editions of Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2, that is currently being exploited in malware attacks.

## NEW BULLETIN SUMMARY

Bulletin Identifier	Microsoft Security Bulletin-1
Maximum Severity Rating	Critical
Impact of Vulnerability	Remote Code Execution
Restart Requirement	The update will require a restart.
Affected Software	Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2.

Note: information on affected software listed above is an abstract. Please see the Advance Notification Web page at the link below for complete details.

The full version of the Microsoft Security Bulletin Advance Notification for August 2010 can be found at <http://www.microsoft.com/technet/security/bulletin/ms10-aug.aspx>.

## PUBLIC BULLETIN WEBCAST

Microsoft will host a webcast to address customer questions on the out of band bulletin on August 2, 2010, at 1:00 PM Pacific Time (US & Canada). Register for the Security Bulletin Webcast at <http://www.microsoft.com/technet/security/bulletin/summary.aspx>.

## RESOURCES RELATED TO THIS ALERT

- Microsoft Security Response Center (MSRC) Blog: <http://blogs.technet.com/msrc/>
- Microsoft Security Research & Defense (SRD) Blog: <http://blogs.technet.com/srd/>
- Microsoft Malware Protection Center (MMPC) Blog: <http://blogs.technet.com/mmoc/>
- Microsoft Security Development Lifecycle (SDL) Blog: <http://blogs.msdn.com/sdl/>

At this time no additional information on this bulletin such as details regarding severity or details regarding the vulnerability will be made available until the bulletin is published.

## REGARDING INFORMATION CONSISTENCY

We strive to provide you with accurate information in static (this mail) and dynamic (Web-based) content. Microsoft's security content posted to the Web is occasionally updated to reflect late-breaking information. If this results in an inconsistency between the information here and the information in Microsoft's Web-based security content, the information in Microsoft's Web-based security content is authoritative.

[Return to Table of Contents](#)

# ***GENERAL OPERATIONAL INFORMATION***

---

## **103.15 CIS PASSWORDS**

CIS passwords expire six months from the date a user changes her password. For example: a user changes her password on 5/13/10; the new password will expire on 11/13/10.

As the date of expiration approaches, workers logging on to CIS are presented with a prompt to generate a new password. This prompt appears for one month, and once it disappears the user will be locked-out of CIS. At that point, access must be restored through contacting the Bureau of Information Services (BIS).

OCDEL understands that while CIS can be an important tool for obtaining information on cases associated with a CAO, CCIS staff with CIS access may not always need to use the system on a regular basis. However, OCDEL recommends that staff log-on to CIS at least *once a month* even if there is not an immediate business need to do so, to prevent users from being locked-out of CIS.

[Return to Table of Contents](#)

[See Manual Section “103.32.3.14 – Questions – 103.15 – CIS Passwords”](#)

## **103.16 DEPARTMENT E-MAIL ACCOUNTS**

Agencies with an Option 1 designation log into CWOPA from their Department-supported desktop computer directly. See [Option 1 CWOPA Accounts](#) for a listing of these accounts.

Agencies with an Option 2 designation do not have direct access to CWOPA. These agencies must log into CWOPA via a Web-Access account. Option 2 sites have been given multiple web-access accounts for business purposes. See [Option 2 CWOPA Web Access](#) for a listing of these accounts.

Agencies using web-access must use a computer connected to the Internet and go to “Outlook Web Access” (OWA) at <https://webmail.state.pa.us/exchweb/bin/auth/owalogon.asp?url=https://webmail.state.pa.us/Exchange/&reason=0&replaceCurrent=1> and enter their user name and password when the website’s logon screen is presented. Instructions for accessing the website can be found in [Instructions for Outlook Web Access](#). An agency using web-access gains admission to CWOPA e-mail, but this method has limitations. Resource Accounts cannot be attached to web-access accounts. Resource accounts are e-mail inboxes that are attached to a main CWOPA account. By logging into a main account, a user has access to these resource accounts.

[Return to Table of Contents](#)

[See Manual Section “103.32.3.15 – Questions – 103.16 – Department E-mail Accounts”](#)



# GENERAL OPERATIONAL INFORMATION

---

## **103.16.1 Granting & Removing Access to Generic Account - Option 1 Sites**

“Generic” CCIS accounts were established to serve as the primary address for the CCIS to receive official communications from OCDEL as well as inquiries from Internet users with questions about the Commonwealth of Pennsylvania Access to Social Services (COMPASS) application process.

A generic address is attached to an office or location, as opposed to an individual. An actual example of a generic address would be [c-yorkcc@pa.gov](mailto:c-yorkcc@pa.gov) (for the York CCIS). E-mail sent to a generic address may be accessed from any Department-supported desktop computer by entering the user name and password for the generic address at the initial logon screen.

Access to an e-mail account may be granted through the “Permissions” function in Microsoft Outlook. This function enables the account to be managed by additional users without the users being required to log-on separately. Access to an e-mail account may be removed also through the “Permissions” function in Outlook.

Option 1 CCISs wishing to manage the generic CCIS e-mail account through single, individual log-on should follow the instructions outlined in [“Granting and Removing Access to the Generic CCIS E-Mail Account”](#).

[Return to Table of Contents](#)

[See Manual Section “103.32.3.16 - Questions - 103.16.1 - Granting & Removing Access to Generic Account - Option 1 Sites”](#)

## **103.16.2 Granting & Removing Access to R&R Account - Option 1 Sites**

Option 1 CCISs wishing to manage the CCIS R&R e-mail account through single, individual log-on should follow the instructions outlined in [“Granting and Removing Access to CCIS R&R E-Mail Account”](#).

[Option 1 R&R Account Names](#) lists the R&R Account Names for Option 1 sites.

The [“Procedure for R&R E-mail Functions”](#) is self-explanatory and provides an overview of use of the R&R e-mail function when sending referral lists and follow-up questionnaires to parents.

[Return to Table of Contents](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.16.3 Accessing Accounts – Option 2 Sites

Option 2 CCISs should continue to follow the instructions outlined in [“Instructions for Web Outlook Access”](#) to access and manage the generic CCIS and R&R e-mail accounts. Because these accounts are accessed and managed through the Internet, separate log-on is still required.

[Option 2 Web Access R&R Accounts](#) highlights the selected R&R e-mail addresses for Option 2 sites. If an Option 2 site requires changing the R&R e-mail address to a different account, notify your Subsidy Coordinator.

[Return to Table of Contents](#)

## 103.16.4 Account Passwords – All Sites

CCIS user may ***NEVER*** give their passwords to anyone. The ***ONLY*** time it is acceptable for a CCIS user to provide someone with his/her username is if the CCIS user is verbally affirming the username while speaking with an authorized information technology professional from the CCIS agency or from the Office of Administration’s Office for Information Technology. Commonwealth information technology professionals will always talk with a CCIS user on the phone and will never ask the CCIS user by e-mail to send a username and/or password.

The following subsections provide additional policy and procedures regarding creating and changing account passwords and lock-outs.

[Return to Table of Contents](#)

[See Manual Section “103.32.3.17 – Questions – 103.16.4 – Account Passwords”](#)

### 103.16.4.1 Creating Passwords

When creating passwords for the generic account, the CCIS should observe the following requirements. The password must:

1. Be at least seven (7) characters in length.
2. Contain characters from at least three (3) of the following categories:
  - a. Upper case letters.
  - b. Lower case letters.
  - c. Numbers.
  - d. Special characters, such as \*, @, #.

[Return to Table of Contents](#)

[See Manual Section “103.32.3.18 – Questions – 103.16.4.1 –Creating Passwords”](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.16.4.2 **Changing Passwords**

When changing passwords for the generic account, the CCIS should remember that:

1. The password must be changed every sixty (60) days or it will expire.
2. The system will prompt the user beginning fourteen (14) days before and every day thereafter leading up to the expiration.
3. The password may be changed more frequently, but no more frequently than every two (2) days, if local need dictates.
4. Once used, a password cannot be re-used for six (6) cycles (changes).

**NOTE:** Due to password expiration, it will still be necessary for the CCIS to periodically log-on to the generic CCIS account to keep the password for that account current. The password for the generic CCIS account must be kept current in order to use the “permissions” function for the account.

[Return to Table of Contents](#)

[See Manual Section “103.32.3.19 – Questions – 103.16.4.2 – Changing Passwords”](#)

## 103.16.4.3 **Lock-outs**

A user will be locked-out after five (5) consecutive invalid log-on attempts.

A log-on attempt will be invalid if:

1. The username and password are not entered exactly as established, with observance to upper and lower case, special characters, etc.
2. The “Num Lock” key on the computer keyboard is not “on”.

**NOTE:** Out of business necessity, more than one CCIS employee might be accessing the generic account on a regular basis. If the CCIS has established this practice, it must remember that invalid log-on attempts will compile at an account level, not an employee level. This means that if one employee performs an invalid log-on attempt, only four “strikes” will be left for any other employees attempting to log-on to the account.

# GENERAL OPERATIONAL INFORMATION

---

The CCIS should follow usual procedures and call the Help Desk when experiencing a lock-out on the generic account.

[Return to Table of Contents](#)

[See Manual Section “103.32.3.20 – Questions – 103.16.4.3 –Lock-outs”](#)

## 103.17 POLITICAL ACTIVITY GUIDELINES

CCIS agencies must be aware of and comply with the guidelines set forth by the CCIS’s parent agency regarding political activities.

[Return to Table of Contents](#)

## 103.18 MILEAGE REIMBURSEMENT

Information regarding mileage reimbursement for CCIS work-related travel necessary outside of regular commuting may be obtained at:  
[http://ocd/custom/ccis/comm/general/docs/GC\\_10-03\\_01.pdf](http://ocd/custom/ccis/comm/general/docs/GC_10-03_01.pdf).

[Return to Table of Contents](#)

## 103.19 ORDERING FORMS & PUBLICATIONS

When an order for forms and publications is received by Headquarters (HQ), it is entered into the publication-ordering system. Orders are entered twice per week. From this point forward – the CCIS agency’s order is in the hands of the Department of General Services (DGS). OCDEL does not print, select, or distribute the orders.

**After the CCIS order is placed by HQ, OCDEL cannot control the speed or accuracy of your order.**

Print on Demand (POD) publication orders take longer to ship than warehoused publications. POD publications are also typically shipped separately from warehoused items.

Backorders happen from time to time. Backorders can sometimes take more than six weeks to be shipped. When available, backorders will be filled by the warehouse.

**There is no need to submit a reorder for the same publications if you do not receive them timely; this complicates the process and you may end up with a double or triple shipment.**

Partial orders typically indicate that either a particular item is on backorder or that one or more of your items are POD and will be shipped separately.

Some publications are available online, via the OCDEL intranet. The CCIS may print verification forms directly from the intranet, rather than placing an order using the [Publication Requisition Form](#):

# GENERAL OPERATIONAL INFORMATION

---

When the CCIS places an order for forms and/or publications, the CCIS must:

1. Use the most recent [Publication Requisition Form](#).
2. Assure requisition forms are legible when sending to HQ.
3. Maintain a reasonable stock of publications (six-week supply is recommended) so you do not run out while waiting for your next shipment.
4. Compile your orders onto one requisition form. Do not submit multiple small orders every-other day. Try to order only one time per month.

**Failure to adhere to the recommended procedures listed above may cause a delay in processing the order.**

[Return to Table of Contents](#)

## 103.20 FAMILY FILE & SUBPOENAS

As set forth in [§ 3041.84](#) (relating to family file), “The CCIS shall establish and maintain a separate file for the family of each p/c who applies for subsidized child care. The family file shall contain documents pertaining to eligibility determination, redetermination, subsidized child care authorization, co-payment agreements and copies of written notices required to [55 Pa.Code, Chapter 3041](#) (relating to subsidized child care eligibility). A p/c or an authorized representative has a right to examine the family file.”

CCIS agencies may determine how to maintain files based on individual operational needs; however, information must be maintained in a consistent manner throughout the CCIS and files must maintain an orderly arrangement of documents that facilitates the case review process. Contents of the files must include all information related to application, eligibility, schedules, reported changes and redeterminations. All information in the file must be date-stamped. CCIS agencies must follow the basic guidelines listed below when establishing and maintaining case files:

1. **Only one case file is necessary.** If the family has participated in multiple funding programs and has more than one County/Record number, OCDEL’s Division of Policy recommends CCIS agencies use color coded pages or a face sheet to indicate the type of case and new case record number.
2. **Maintain most current information on top of the file.** The oldest information should be at the bottom of the file.
3. **All information documenting a specific application or redetermination must be kept together in a systematic manner so each eligibility period is separate and easily identified.**
4. **Breaks in eligibility segments should be apparent.** CCIS agencies can choose to distinguish separate eligibility segments by using a color coded face page, colored tabs or “post it” labels, staples or clips. Information regarding the current eligibility segment should be on top.

# GENERAL OPERATIONAL INFORMATION

---

5. **File “one time only” information with the current application or in a specific section of the file folder.** HIPPA forms, Release of Information, photo- identification and other types of “one time only” verifications should be easily identifiable and accessible within the file.
6. **Mark documentation that is used to verify multiple eligibility segments so it is easily located.** Previously obtained Employment Verification forms, support information and other types of documentation that continue to support current eligibility should be flagged with tabs, labels or “post it” notes. Temporary tabs, labels or “post it” notes allow workers to easily remove and re-mark new documentation as it is submitted, so the current verifications are always easily identifiable.
7. **Temporary Assistance for Needy Families (TANF) files.** The County Assistance Office (CAO) is the eligibility agent for TANF child care. As a result, TANF case files contain little documentation. At a minimum, each TANF case file must contain a TANF/FS/SNAP/GA/WS2 Self-Certification form. A copy of photo-identification or other proof of the p/c’s identity should be in the file. TANF files must also include documentation of a child’s disability when appropriate. Please refer to the Forms and Publications segment of the OCDEL Intranet for current TANF/FS/SNAP/GA/WS2 Self-Certification forms.
8. **PELICAN CCW is the formal record keeping system.** It is not necessary for the CCIS to print screen shots, notices or forms on a regular basis.
9. **All information entered into PELICAN CCW must be documented clearly in the hard file.**

**EXCEPTION:** There is no need to keep case comments, including those noting collateral contacts, in the hard file unless the comments are related to special circumstances (i.e., domestic violence, very young teen parents or CCMIS employees receiving subsidized child care services).

Information contained in the family file is restricted to individuals connected with the administration of the Subsidized Child Care Program. Any member of the family or authorized person acting on behalf of the family, **including advocates or legal representatives**, may review the family file during the CCIS agency’s regular operating hours. A person other than those identified above may be permitted to access a family file only with the p/c’s written permission. All case information is considered confidential. There are some circumstances, which require the CCIS to take additional steps to further safeguard information. When a case meets any of the following conditions the CCIS must keep case comments in the hard file only (i.e., not within PELICAN CCW) and the hard file must be kept separate from other case files in a location that is secured and is accessible only by the Director or a designee of the Director’s choice. Cases requiring special confidentiality measures include the following:

1. A teen parent who is 13 years of age or younger.
2. An employee of the CCIS.
3. An individual who has disclosed circumstances, which include domestic or other violence.

Subsidy Coordinators will require CCIS agencies with poorly maintained files to submit a plan for consistent file maintenance in writing. Information that is not readily available will be marked as missing in subsequent reviews. If the CCIS needs help with creating a filing system, your Subsidy Coordinator can offer several options that they have found to work well in other agencies.

# GENERAL OPERATIONAL INFORMATION

---

When presented with a subpoena, the CCIS **MAY NOT** release information about the p/c and/or the p/c's child(ren). The CCIS may release information regarding providers, such as the total number of children formerly receiving subsidy, the total number of children currently receiving subsidy and the total amount of subsidy paid to the provider. However, unless the case relates to a form of welfare fraud, the CCIS **MAY NOT** release information regarding a current subsidy recipient unless presented with a court order or a written authorization signed by the p/c.

**NOTE:** CCIS agencies must work cooperatively with the Office of Inspector General (OIG) and share current client information with the OIG as it pertains to their investigation.

When presented with a subpoena requesting information about a current subsidy recipient, the CCIS should respond in writing using the [CCIS Response to Subpoena](#) document.

[Return to Table of Contents](#)

[See Manual Section "103.32.3.21 – Questions – 103.20 – Family File & Subpoenas"](#)

## 103.21 **RECORD RETENTION**

**As set forth in § 3041.85 (relating to record retention), "The CCIS shall retain family files, completed application forms, written notices, books, records and other fiscal and administrative documents pertaining to subsidized child care. Records shall be maintained for at least 6 years from the end of the fiscal year in which subsidized child care has been provided or until an audit or litigation is resolved. The fiscal year is a period of time beginning July 1 of any calendar year and ending June 30 of the following calendar year."**

The CCIS and its subcontracted providers shall maintain books, documents and other records pertaining to the costs and expenditure of subsidized child care funds to reflect all costs and expenses for the operation of the Subsidized Child Care Program. Books, records, and documents shall be maintained according to generally accepted accounting principles using the accrual method of accounting.

The CCIS and subcontracted providers shall retain the following: family files, ineligible application forms, information and referral logs, books, records, OIG review & cases, and other fiscal and administrative documents pertaining to expenditures of subsidized child care funds.

The above list of documents and records must be kept for six years from the end of the fiscal year in which the activities occurred or until an audit or litigation is resolved, whichever occurs last.

**NOTE:** CCIS agencies must keep files of staff members who are receiving funds from the subsidized child care program locked in a file that can only be accessed by executive director.

[Return to Table of Contents](#)

[See Manual Section "103.32.3.22 – Questions – 103.21 – Record Retention"](#)



# ***GENERAL OPERATIONAL INFORMATION***

---

## **103.22 REPORTING CHILD ABUSE**

As set forth in [§ 3041.86](#) (relating to child abuse reporting), “The CCIS shall immediately report suspected child abuse in accordance with 23 Pa.C.S. §§ 6301—6385 (relating to the Child Protective Services Law) and [Chapter 3490](#) (relating to child protective services).”

CCIS and volunteer workers are mandated reporters and must report all suspected child abuse. For any suspected child abuse the CCIS will contact:

- Childline, the State Child Abuse Hotline (1-800-932-0313); or
- The county children and youth agency where the alleged abuse occurred.

[Return to Table of Contents](#)

[See Manual Section “103.32.3.23 – Questions – 103.22 – Reporting Child Abuse”](#)

## **103.23 PROVIDER COMPLAINTS**

The CCIS should encourage a p/c to report a complaint about a child day care facility first-hand to the appropriate Regional OCDEL Office. If the p/c fails to do so the CCIS must report the complaint to the appropriate Regional OCDEL Office, based upon the information in the [Regional Child Development Offices and Map](#).

[Return to Table of Contents](#)

[See Manual Section “103.32.3.24 – Questions – 103.23 – Provider Complaints”](#)

## **103.24 WORKING WITH OTHER AGENCIES**

The CCIS will:

- Establish ongoing working relationships with other county service agencies; school districts; intermediate units; domestic violence programs; and the Domestic Relation Sections of the courts.
- Appoint a staff person to work directly with the CAO to ensure that all funding available for subsidized child care is made available to and utilized by an eligible p/c. Such networking will help prevent duplication of services, and will assure continued service to eligible families without regard to the funding source.

[Return to Table of Contents](#)



# ***GENERAL OPERATIONAL INFORMATION***

---

## **103.24.1 PA Key**

CCIS agencies have always played a key role in partnering with local and state early care and education groups. This continued partnership is essential in helping to identify and fill child care gaps, improve the quality of care and better meet the needs of families.

The CCIS agencies and the PA Keys work together to develop an understanding and monitor early care and education in their communities. Together, these groups offer services and planning expertise to help families and communities with their early care and education needs and to proactively address service gaps and demand.

The CCIS must maintain regular contact and collaborate with its Regional Key Office in meeting the early education needs of families and communities.

This collaboration should include, but not be limited to:

1. Participating as a hub to promote widespread parental knowledge of Keystone STARS. This work involves cooperation and proactive coordination with the Regional Keys.
2. Working proactively with groups that support the Keys to promote early learning services that will benefit children and families in their community.
3. Identifying p/c and provider information needed to complete community needs assessments which is available at CCIS agencies through reports generated from PELICAN CCW.
4. Keeping informed of public education activities and events.

[Return to Table of Contents](#)

[See Manual Section “103.32.3.25 – Questions – 103.24.1 – PA Key”](#)

## **103.24.2 County Assistance Office (CAO)**

The CCIS must develop and maintain collaborative relationships with the local CAO through the assigned CAO Liaison and with the Employment & Training (E&T) contractors in order to effectively deliver child care benefits to families who receive TANF, GA/WS2 and/or FS/SNAP benefits through the Office of Income Maintenance (OIM).

Demographic and eligibility information pertaining to a family receiving TANF, GA/WS2 and/or FS/SNAP benefits is transferred to PELICAN CCW from the Client Information System (CIS), the computer information system used by the CAO to determine eligibility for TANF and FS/SNAP benefits.

# GENERAL OPERATIONAL INFORMATION

---

The CAO uses CIS to determine eligibility for TANF and FS/SNAP benefits and the child care related to those benefits. The CAO uses CIS to do the following:

1. Determine initial and continuing eligibility for TANF, GA/WS2 and/or FS/SNAP and for child care related to these programs.
2. Determine household composition, employment and training participation, income and financial eligibility.
3. Process reported changes in household composition, employment and training, and income.
4. Refer a p/c to the CCIS to receive help with locating quality child care and assistance in paying child care costs.

The CCIS *must* have an “Open Door” policy with regard to a p/c’s report of a change. If a p/c reports a change that affects eligibility, the CCIS will do everything possible to assist the p/c in reporting this change to the CAO via making a phone available to call the [Statewide Customer Service Center \(SWCSC\)](#) or faxing the verification to the CAO. If a p/c insists that the information in CIS is incorrect and has not yet been updated (i.e., the p/c ended employment but CIS and PELICAN CCW still reflect a paid activity and thus a co-payment (co-pay) when a co-pay should no longer be assessed) and the incorrect information is causing a hardship for the p/c, the CCIS may contact their CAO Liaison to discuss the situation, determine next steps and reach agreement regarding timeframes for resolution. If the situation cannot be resolved, the CCIS must contact their Subsidy Coordinator to report the issue.

[Return to Table of Contents](#)

## **103.24.3 Employment & Training (E&T) Contractors**

The CCIS will have contact with Employment & Training (E&T) programs contracted by the Department to provide employment and training services for individuals working with the CAO to achieve self-sufficiency and diminish reliance upon welfare. E&T contractors serve individuals in geographic service regions known as Workforce Investment Areas (WIAs) designated by the Pennsylvania Department of Labor & Industry. In many instances, one WIA serves multiple counties. Under the Workforce Investment Board (WIB) for that county or region, the Local Management Committee (LMC) maintains specific oversight of E&T contracted programs to insure progress and compliance. The LMC meets regularly to discuss the progress of CAO clients and the needs of the local community. Core members of the LMC include representatives from the CAO and the local education and business communities. CCIS agencies are strongly encouraged to make contact with the local WIB and participate in LMC meetings.

[Return to Table of Contents](#)

[See Manual Section “103.32.3.26 – Questions – 103.24.3 – E&T Contractors”](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.24.4 **Regional OCDEL Offices**

All CCIS agencies must have available a copy of 55 Pa. Code, Chapters **3041** (relating to subsidized child care eligibility), **3270** (relating to child day care centers), **3280** (relating to group child day care homes) and **3290** (relating to family child day care homes).

The CCIS should encourage a p/c to report a complaint about a child day care facility first hand to the appropriate Regional OCDEL Office. If the p/c fails to do so the CCIS must report the complaint to the appropriate Regional OCDEL Office, based upon the information in the **Regional Child Development Offices and Map**. The map and contact information for the Regional OCDEL Offices, “Regional Child Development Offices and Map” is also available under “**Contact Lists**” on OCDEL’s intranet site.

The CCIS must refer to the following contact information when an issue is encountered that necessitates coordination with the Regional OCDEL Offices:

- **Provider Type Changes (Regulated to Unregulated)** –  
When a regulated provider who uses their Social Security Number for their Tax ID needs to be reopened, the CCIS can contact OCDEL Policy through **RA-cmissedsupport@pa.gov**. The CCIS must make sure the regulated provider is closed by the Regional Office and must send an e-mail to the above e-mail address that includes the provider’s date of birth with the request to reopen the Legal Entity and Location as an R/N.
- **Critical PELICAN Provider Payment Issues** –
  1. The CCIS first contacts the Subsidy Coordinator to explain the issue.
  2. The Subsidy Coordinator will discuss the issue with regional Certification staff to try to resolve the issue.
  3. If the Subsidy Coordinator cannot solve the concern easily, the CCIS then calls the Help Desk so a PCR can be entered to address the problem.

**[Return to Table of Contents](#)**

**[See Manual Section “103.32.3.27 – Questions – 103.24.4 – Regional OCDEL Offices”](#)**

# ***GENERAL OPERATIONAL INFORMATION***

---

## **103.24.5 Internal Revenue Service (IRS)**

The CCIS must share information on the Earned Income Tax Credit (EITC) with families participating in the subsidized child care program and issue the Internal Revenue Service (IRS) Form 2333TE “SPEC Outreach Order Form”. The EITC is a credit that helps working families with low to moderate incomes keep more of what they work for. It helps to reduce taxes and, in some instances, may mean a refund.

The CCIS must inform families participating in the subsidized child care program about the availability of this tax credit. The IRS has several publications that contain helpful information on the EITC.

Publications are available and may be ordered at no cost to the CCIS via the [IRS Order Form SPEC 2333TE](#). The CCIS should use this form to order EITC and other publications each tax year by completing it, printing it and then sending it to Mr. George C. McGriff.

E-mail [George.C.McGriff@irs.gov](mailto:George.C.McGriff@irs.gov) or

FAX 215-861-1116

The preferred method to return the form is electronically. If the CCIS is unable to submit the form electronically, the form may be faxed to George C. McGriff’s attention. For more information on

[Return to Table of Contents](#)

[See Manual Section “103.32.3.28 – Questions – 103.24.5 – IRS”](#)

## **103.24.6 Office of the Inspector General (OIG)**

The CCIS must refer cases to the OIG in the following circumstances:

1. Up-front investigations.
2. Ongoing questions and/or concerns regarding a failure to comply with eligibility and/or reporting requirements.
3. Suspected fraud by a p/c and/or provider.
4. Inability to initiate or complete collection of the total amount of an overpayment.

The CCIS must refer to [Manual “412 – Client Overpayment & Recovery”](#).

[Return to Table of Contents](#)

# ***GENERAL OPERATIONAL INFORMATION***

---

## **103.24.7 Office of Children, Youth and Families (OCYF) & Sharing Information regarding Keystone STARS Placements**

This subsection provides information regarding the CCIS agencies' responsibilities when working with OCYF and guidelines for the use of Needs-Based Funding (NBF) to purchase child care for children involved with county Children and Youth services (CYS) agencies.

Any CYS that chooses to use NBF to pay for child care must do the following:

1. Explore the family's eligibility for Child Care Works (CCW) and require eligible families to apply for subsidized child care.
2. Enroll children in facilities with a Keystone STARS quality rating of 2 and above.
3. Use provider rates set by OCDEL.

NBF may be used to pay for child care while parents, foster parents and teen parents eligible for CCW, wait for funding to become available. CYS may also use NBF to pay for child care for families that need child care but are not eligible for CCW.

NBF may only be used to pay for care with providers that have a Keystone STARS quality rating of 2 and above. In rare instances, a STARS 2 or above facility may not be available or accessible. In that case the CYS must request an exemption from OCYF Headquarters that will be reviewed by both OCYF and OCDEL prior to granting permission to use a one STAR or no STARS facility. CYS must resubmit requests for exemptions every six months if the need continues to exist.

CYS may not use NBF to pay for care in unregulated homes.

CYS must pay the provider rates established by OCDEL. The CYS will pay the providers published rate or the Maximum Child Care Allowance (MCCA), whichever is less. CYS will also pay the STARS add-on rate.

CCIS agencies must provide their local CYS with provider rate information and lists of STARS 2 and above providers. The CCIS must also assist CYS families with the application process and provide R&R services as needed.

**[Return to Table of Contents](#)**

**[See Manual Section "103.32.3.29 – Questions – 103.24.7.2 – Sharing Information regarding Keystone STARS Placements"](#)**

# ***GENERAL OPERATIONAL INFORMATION***

---

## **103.25 HELPLINE**

The Department has established a single statewide toll-free number that families can call to obtain information on child care. The toll-free number is 1-877-4PA-KIDS or 1-877-472-5437. The toll-free HELPLINE staff are located in Harrisburg and will operate from 8:30 a.m. until 5:00 p.m., five days per week, Monday through Friday.

HELPLINE staff are prepared to provide the following types of information:

1. Contact information for each CCIS for help locating a child care provider.
2. Information regarding how to obtain assistance in paying for child care.
3. Information regarding how to work with a child care provider to ensure a child is receiving quality early learning opportunities.
4. Information regarding the status of a child care facility's license or how to submit a complaint regarding a specific child care provider.
5. Information regarding other Department programs and services for families, such as Children's Health Insurance Program (CHIP), Women Infant Children (WIC), Early Childhood Education Linkage System (ECELS), Poison Information Center and the Child Abuse Hotline.

HELPLINE's role is not to duplicate the tasks of the CCIS regarding R&R services, but rather to direct callers to the correct location so the caller may obtain needed information. The HELPLINE is an agent of the Department so it is not a breach of confidentiality for the CCIS to share information with HELPLINE staff about a family's eligibility for subsidy. The CCIS must provide information regarding a family's eligibility to HELPLINE staff upon request.

The CCIS must take the following steps to ensure an effective working relationship with the HELPLINE:

1. Designate a "contact person" for calls from the HELPLINE.
2. Attempt to resolve the issue with the p/c and then contact the HELPLINE to confirm how the issue was resolved, when the CCIS receives a call from the HELPLINE that requires additional contact with a p/c.

[Return to Table of Contents](#)

[See Manual Section "103.32.3.30 - Questions - 103.25 - HELPLINE"](#)

## **103.26 HELP DESK**

The PELICAN CCW Help Desk was established to help CCIS agencies troubleshoot system-related problems.

CCIS designated callers may contact the Help Desk between the hours of 8:30 a.m. and 4:30 p.m., Monday through Friday.

**EXCEPTION:** CCIS designated callers should report slow system response and system unavailability issues as soon as they occur, regardless of the date/time.

# GENERAL OPERATIONAL INFORMATION

The CCIS should continue to work with the local CAO to resolve data discrepancies in CIS. If the CAO is not able to correct or change the data in CIS, the CAO should contact the CIS Hotline. **Help Desk cannot assist with these problems and cannot contact the CIS Hotline.**

Also, the CCIS should continue to direct questions or issues related to policy to the assigned Subsidy Coordinator. The Subsidy Coordinator continues to be the “first line of defense” for the CCIS for these and other non-system issues.

Guidelines for contacting the Help Desk are listed in the [PELICAN CCW Troubleshooting Guide](#) document.

[Return to Table of Contents](#)

[See Manual Section “103.32.3.31 – Questions – 103.26 – Help Desk”](#)

## 103.27 **STAFFING, TRAINING NEEDS & COORDINATION**

The CCIS is required to employ individuals receiving public assistance from the Department and to submit quarterly reports ([Form PA 1540](#)) of hiring under the CCIS plan for recruiting and hiring public assistance recipients ([Form PA 778](#)). In order to comply with this requirement, each grantee must complete and submit a plan for recruiting and hiring of public assistance recipients for employment ([Form PA 778](#)) under the CCIS grant. Then, when the plan is approved, the grantee is to make a good faith effort to fill at least 25% of the new/vacant jobs under the grant with qualified recipients referred by the CAO Employment Unit Coordinator. Hiring under the approved plan is to be verified by submitting a Quarterly Contract Report ([Form PA 1540](#)). The ongoing schedule for reporting is as follows:

<b><i>Reporting Period</i></b>	<b><i>Report Due Date</i></b>
January 1 – March 31	April 15th
April 1 – June 30	July 15th
July 1 – Sept 30	October 15th
Oct 1 – Dec 31	January 15th

Questions regarding the plan, the quarterly reporting requirement and/or [Form PA 1540](#) can be directed to the Contractor Partnership Program by calling toll-free 1-866-840-7214, Monday through Friday from 9:00 a.m. to 4:30 p.m. or by e-mailing [ra-betpcpp@pa.gov](mailto:ra-betpcpp@pa.gov).

The mailing address where the quarterly employment reports must be sent is:

OIM/Bureau of Employment and Training Programs (BETP)  
Health & Welfare Building, 2nd Floor – West,  
7th & Forster Street Harrisburg, PA 17105.

The CCIS must also send a copy to OCDEL at 333 Market Street, Sixth Floor Harrisburg, Pennsylvania 17126; ATTN: Subsidy

The CCIS must ensure all work is supervised for accuracy and timeliness to assure that all aspects of the workplan, regulations pertaining to 55 PA Code, Chapters **3041** (relating to subsidized child care eligibility) and **168** (relating to child care), the CCIS Policy & Procedures Manual, Performance Standards and other correspondence from the Department are met.



# **GENERAL OPERATIONAL INFORMATION**

---

The CCIS must meet the following criteria regarding staff training:

1. New staff must be trained within 60 calendar days of their start date for all aspects of their job assignments.
2. Staff must receive ongoing training within 30 calendar days of updates or changes to any aspect of their job assignments.
3. Staff must be cross-trained to assure that core functions are able to be performed in the event of staff vacancies and/or absences.
4. A training plan is established indicating how criteria set forth in (1) through (3) above will be met.

Additional information regarding staffing, training needs and coordination is set forth in [Manual "100 - Grants & Subcontracting"](#).

[Return to Table of Contents](#)

[See Manual Section "103.32.3.32 - Questions - 103.27 - Staffing, Training Needs & Coordination"](#)

## **103.28 OCDEL RESPONSIBILITIES**

OCDEL is responsible to ensure that regulated child care providers are in compliance with all regulations set forth in 55 Pa. Code, Chapters [3270](#), [3280](#) and [3290](#) (relating to the child day care centers; group child day care homes and family child day care homes). Also included are those providers who are exempt under Chapters [3270](#), [3280](#) and [3290](#) and who meet certain funding standards set forth by the Department.

OCDEL must:

1. Enter into a grant with a legal entity to operate the CCIS in each county to manage the Subsidized Child Care Program.
2. Distribute available funding in an equitable manner, according to certain county demographics and/or the historic utilization of funds in that county.
3. Establish county-specific maximum child care allowance rates by service type.
4. Make available and support a software package for the management of the subsidized child care program.
5. Reimburse the CCIS according to the provisions of the grant.
6. Provide technical support as needed to the CCIS.
7. Hold meetings and training sessions as needed.
8. Monitor the grant through performance standard reviews.

[Return to Table of Contents](#)



# ***GENERAL OPERATIONAL INFORMATION***

---

## **103.29 CCIS RESPONSIBILITIES**

The CCIS's responsibilities are outlined each year in the grant between the CCIS and the Department.

The following are the CCIS responsibilities regarding the subsidized child care program:

1. Use the Departmental issued software (i.e., PELICAN CCW) to manage the subsidized child care program.
2. Provide R&R services and distribute child care information to a p/c who is seeking child care services as set forth in **Manual "200 - R&R"**.
3. Attend all meetings and training sessions held by the Department.
4. Not impose additional charges to a subsidy-eligible family for services provided under the provisions of the grant with the Department.
5. Ensure that each county resident may access the CCIS from their home residence by telephone without a long distance charge.
6. Assure neutrality by offering a p/c a comprehensive unbiased selection of available child care programs and providers.
7. Actively promote and publicize the parent-choice system to county residents and providers.
8. Coordinate with other funding agencies to maximize the utilization of all available child care funding and development of a seamless funding system.
9. Develop a plan for the initial training of staff.
10. Develop a system that assures accuracy, timeliness and accountability in the following areas:
  - a. Client access.
  - b. Neutrality in making management decisions.
  - c. Neutrality in providing child care options.
  - d. Compliance with regulations, Department policies and grant conditions.
  - e. Financial stability of the CCIS.
  - f. Encumbrance and expenditure control.
  - g. Use of funds for allowable expenses and eligible children.
11. Develop a plan to manage heavy enrollment periods and for summer programs when additional children are being funded and school-age children move from part-time to full-time funding.
12. Develop a plan to monitor the provider's collection of co-payments and reporting of absences.
13. Develop a plan to monitor enrollment of subsidized children in the child care facility.
14. Monitor the administrative budget to ensure that funds are being spent according to the approved grant and in accordance with the Allowable Cost Guidelines.

# GENERAL OPERATIONAL INFORMATION

---

15. Request in writing advance approval to relocate the CCIS agency at least 45 days prior to a tentative relocation. Additionally, the Grantee will request in writing advance approval to expand space or any other change that will permanently increase occupancy expenses to the CCIS budget during the grant period.
16. Determine the eligibility of a family who is seeking child care services according to the regulation stated in 55 Pa.Code, Chapter [3041](#).
17. Establish an agreement with a child care provider to participate in the subsidized child care program.
18. Verify reimbursement rates of a participating provider as set forth in [Manual "305 - Provider Payment"](#).
19. Assist in the payment of child care services for an eligible child.
20. Monitor a provider to ensure that the provider is:
  - a. Collecting the assessed weekly co-payment.
  - b. Reporting absences in accordance with 55 Pa. Code, Chapters [168](#) (relating to child care) and [3041](#) (relating to subsidized child care eligibility).
21. Maintain a family file for each participating family as set forth in [§ 3041.84](#) (relating to family file).
22. Generate reports as set forth in [Manual "600 - Reports"](#).
23. Generate correspondence as set forth in [Manual "500 - Correspondence"](#).
24. Manage allocated funds within established guidelines.
25. Reimburse a provider by the 20<sup>th</sup> day of the month following the month of service.
26. Communicate information on child care issues from the Department to a participating child care provider.
27. Maintain a working relationship with other agencies as set forth in [Manual Section "103.24 - Working with other Agencies"](#).
28. Process cases in which a p/c reports domestic or other family violence as set forth in [Manual "415 - Domestic & Other Family Violence"](#).
29. Refer all family files and provider files to the OIG who are suspected of fraudulently receiving subsidized child care funding as set forth in [Manual "412 - Client Overpayment & Recovery"](#) and [Manual "306 - Provider Overpayment & Recovery"](#).
30. Cooperate in ongoing fraud investigations as set forth in [Manual "412 - Client Overpayment & Recovery"](#).
31. Process disqualifications as set forth in [Manual "413 - Disqualification"](#).
32. Process appeals as set forth in [Manual "414 - Appeal & Fair Hearing"](#).

[Return to Table of Contents](#)

# ***GENERAL OPERATIONAL INFORMATION***

---

## **103.30 Using PELICAN CCW**

The PELICAN platform is the Department's integrated solution for supporting the delivery and management of child care and early learning programs under OCDEL. The CCW component of PELICAN helps track, qualify, and enroll clients who are receiving subsidized child care services. The CCIS will use the Departmentally-issued software package, PELICAN CCW, to do the following:

1. Management of workloads (caseloads/providerloads/fiscal loads).
2. Management of workload supervisory units.
3. Offer referral information to any p/c needing help locating a child care provider or early learning program.
4. Process applications for subsidized child care.
5. Complete eligibility determinations and redeterminations.
6. Manage a waiting list for subsidized child care.
7. Track funding encumbered and expended for enrolled children.
8. Project funds available for additional enrollments.
9. Maintain information on each eligible family.
10. Process reported changes and complete ongoing case maintenance activities.
11. Maintain provider files.
12. Generate correspondence, as set forth in regulation and policy.
13. Generate reports required by the Department.
14. Calculate payments to providers.

For additional information regarding use of PELICAN CCW, see [Manual "104 – Use of PELICAN CCW"](#).

[Return to Table of Contents](#)

# GENERAL OPERATIONAL INFORMATION

## 103.31 UPDATED INFORMATION & ADDITIONAL RESOURCES

This section contains a listing of updated information distributed following issuance of this manual section via Announcements, Updates and Communiqués, as well as additional resources available to the CCIS.

### 103.31.1 Announcements

DATE ISSUED	ANNOUNCEMENT NUMBER	TITLE

[Return to Table of Contents](#)

**GENERAL OPERATIONAL INFORMATION**

103.31.2 Updates

DATE ISSUED	UPDATE NUMBER	TITLE

[Return to Table of Contents](#)

## ***GENERAL OPERATIONAL INFORMATION***

---

### 103.31.3 Communiqués

<b>DATE ISSUED</b>	<b>COMMUNIQUE NUMBER</b>	<b>TITLE</b>

[Return to Table of Contents](#)

# GENERAL OPERATIONAL INFORMATION

## 103.31.4 Additional Resources

DATE ISSUED	COMMUNIQUE NUMBER	TITLE

[Return to Table of Contents](#)

# **GENERAL OPERATIONAL INFORMATION**

---

## **103.32 TRAINING GUIDE**

This section contains information pertinent to training the General Operational Information Manual Section. The following subsections contain the goals and objectives of the manual section, as well as helpful question and answer checkpoints.

### **103.32.1 Goals**

The information in this section contains the goals with regard to general CCIS operations. The following are the goals of this manual section:

1. To efficiently and effectively manage the subsidized child care program.
2. To efficiently and effectively perform the CCIS responsibilities.

[Return to Manual Section "103.3 – Goals & Objectives"](#)

### **103.32.2 Objectives**

The information in this section contains the objectives with regard to general CCIS operations. The following are the objectives of this manual section:

1. To list the subsidized child care program objectives and recite the Mission Statement.
2. To identify and effectively use the resources available to the CCIS agencies.
3. To ensure staff are available to the public as set forth in this manual section.
4. To comply with the requirements associated with the following:
  - a. Nondiscrimination.
  - b. Confidentiality.
  - c. HIPAA.
  - d. LEP.
  - e. Use of IT Resources.
5. To effectively manage the CIS and Department e-mail accounts.
6. To effectively and efficiently work with other agencies.
7. To maintain a family file and ensure the record retention requirements are met.

[Return to Manual Section "103.4 – Funding"](#)



# GENERAL OPERATIONAL INFORMATION

---

## 103.32.3 Section Checkpoint Questions

The Policy and Operations Divisions of the Bureau of Subsidized Child Care Services developed the following questions as a checkpoint to ensure comprehension of the information presented within this manual section. Upon review of the information within this section, CCIS staff should be able to answer all of the questions listed below.

### 103.32.3.1 Questions- 103.5 - Subsidized Child Care Program Objectives

1. List the Department's overall objectives for the subsidized child care program.

a. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

b. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

c. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

d. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

e. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

f. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

[Return to Table of Contents](#)

[Return to Manual Section "103.5 - Subsidized Child Care Program Objectives"](#)

[See Answers](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.32.3.2 Questions- 103.9 - Public Access

2. TRUE or FALSE. The CCIS must be open for business and physically present to answer subsidized child care questions from the general public between the hours of 8:30 a.m. and 5:00 p.m., Monday through Friday, except on state-recognized holidays or in the case of County Government managed programs, county-recognized holidays.
3. TRUE or FALSE. The CCIS must establish weekend hours so it is accessible to a p/c and/or provider who cannot contact the agency during the weekday office hours.
4. YES or NO. May the toll-free telephone line have voice-mail as the primary mechanism for handling incoming telephone calls between the hours of 8:30 a.m. and 5:00 p.m., Monday through Friday, except on state-recognized holidays or in the case of County Government managed programs, county-recognized holidays?
5. The CCIS must ensure that each of its staff responds to voice-mail messages within how many working days? \_\_\_\_\_

[Return to Table of Contents](#)

[Return to Manual Section "103.9 - Public Access"](#)

[See Answers](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.32.3.3 Questions- 103.11 - Confidentiality

6. Under which of the following circumstances must the CCIS take additional steps to further safeguard information?

a. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

b. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

c. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

[Return to Table of Contents](#)

[Return to Manual Section "103.11 - Confidentiality"](#)

[See Answers](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.32.3.4 Questions- 103.12 - HIPAA

7. Protected Health Information (PHI) may be disclosed under the following circumstances?
  - a. When the Privacy Rule permits or requires.
  - b. When the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.
  - c. When Health and Human Services (HHS) is undertaking a compliance investigation, review or enforcement action.
  - d. When responding to a subpoena requesting the information.
  - e. (a) through (c) only.
  - f. All of the above.

[Return to Table of Contents](#)

[Return to Manual Section "103.12 - HIPAA"](#)

[See Answers](#)

## 103.32.3.5 Questions- 103.13 - LEP

8. The CCIS may contract with whom in order to assist in working with persons with Limited English Proficiency (LEP)?

---

---

---

---

---

---

---



# GENERAL OPERATIONAL INFORMATION

---

## 103.32.3.6 Questions- 103.14 - Acceptable Use of IT Resources

11. List examples of Commonwealth IT resources.

a. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

b. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

c. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

[Return to Table of Contents](#)

[Return to Manual Section "103.14 - Acceptable Use of IT Resources"](#)

[See Answers](#)

## 103.32.3.7 Questions- 103.14.2.2 - Expectation of Privacy - Internet

12. TRUE or FALSE. All user activity involving internet use is subject to tracking, blocking, logging, auditing, monitoring, accessing, retrieving and reviewing by the Department.

[Return to Table of Contents](#)

[Return to Manual Section "103.14.2.2 - Expectation of Privacy - Internet"](#)

[See Answers](#)

# GENERAL OPERATIONAL INFORMATION

---

## **103.32.3.8      Questions- 103.14.3.1 - Expectation of Privacy - E-mail**

13. When sensitive material is sent electronically via e-mail, it is important to do what?

---

---

---

14. When it is necessary to transmit Commonwealth proprietary or restricted information beyond the Commonwealth Connect e-mail network, how must the messages be protected?

---

---

[Return to Table of Contents](#)

[Return to Manual Section "103.14.3.1 - Expectation of Privacy - E-mail"](#)

[See Answers](#)

## **103.32.3.9      Questions- 103.14.3.4 - Security Issues**

15. How does a CCIS user secure his/her desktop?

---

---

---

[Return to Table of Contents](#)

[Return to Manual Section "103.14.3.4 - Security Issues"](#)

[See Answers](#)

## **103.32.3.10      Questions- 103.14.3.6 - Encryption**

16. An email must be encrypted under what circumstances?

---

---

---

[Return to Table of Contents](#)

[Return to Manual Section "103.14.3.6 - Encryption"](#)

[See Answers](#)





# GENERAL OPERATIONAL INFORMATION

19. Use the screen shots below to answer the question.



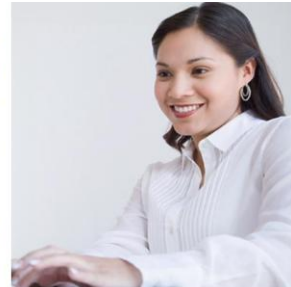
Toni received a strange e-mail at work.

The subject was blank.

The sender had a non-commonwealth e-mail address.

She thought she recognized the sender's name.

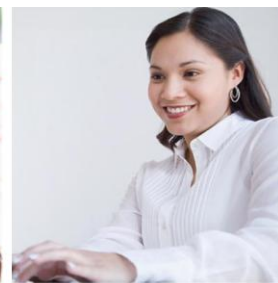
She was expecting important information from a vendor, so she opened the message and its attachment.



It wasn't from the vendor but it said it was from the "IT department" and that a system cleanup was taking place.

It asked for her name, position, user name and password.

Being a conscientious employee, she filled out the attachment and sent it back.



Is this a problem?

**YES**

**NO**

20. Referring to the screen shots in the question above, explain the concerns you have?

---



---



---



---



---



---



---



---



---



---



---

# GENERAL OPERATIONAL INFORMATION

21. Use the screen shots below to answer the question.



“Nice to see you, Kyle.

Can I borrow your phone?

I need to make a quick call to the office.”

“Why do you need to borrow mine, Stacy?”

I thought you had a commonwealth-issued BlackBerry.”



“I do.

But I left it on the seat of my car when I ran into the store.

Somebody took it—can you believe that?”



“Did you report it to the agency’s information technology office?”



“Not yet.

I’ve been managing to get things done without it.

I’ll let them know when I’m back in the office next week.”



Is this a problem?

YES

NO

# GENERAL OPERATIONAL INFORMATION

---

22. Referring to the screen shots in the question above, explain the concerns you have?

---

---

---

---

---

---

---

---

[Return to Table of Contents](#)

[Return to Manual Section "103.14.4 – Unacceptable Use of IT Resources"](#)

[See Answers](#)

## 103.32.3.12 Questions- 103.14.5 - Data Cleansing & Disposal of IT Resources

23. TRUE or FALSE. Peripheral storage devices including but not limited to floppy diskettes, CD and DVD discs along with external storage devices such as USB drives, may be used by end users for storing Commonwealth data.

[Return to Table of Contents](#)

[Return to Manual Section "103.14.5 – Data Cleansing & Disposal of IT Resources"](#)

[See Answers](#)

## 103.32.3.13 Questions- 103.14.6 -Desktop & Server Software Patches

24. What must a CCIS do at the end of the day with his/her computer?

---

---

---

---

---

[Return to Table of Contents](#)

[Return to Manual Section "103.14.6 – Desktop & Server Software Patches"](#)

[See Answers](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.32.3.14 Questions- 103.15 -CIS Passwords

25. CIS passwords expire following what period of time?
  - a. 60 days.
  - b. 6 months.
  - c. 1 year.
  
26. How often does OCDEL recommend CCIS staff log-on to CIS? \_\_\_\_\_

[Return to Table of Contents](#)

[Return to Manual Section "103.15 - CIS Passwords"](#)

[See Answers](#)

## 103.32.3.15 Questions- 103.16 - Department E-mail Accounts

27. Which of the following is an ***INCORRECT*** statement?
  - a. Option 1 sites may log into CWOPA from their Department-supported desktop computer directly.
  - b. Option 2 sites do not have direct access to CWOPA and must log into CWOPA via a Web-Access account.
  - c. There is no difference between Option 1 and Option 2 sites when accessing CWOPA.

[Return to Table of Contents](#)

[Return to Manual Section "103.16 - Department E-mail Accounts"](#)

[See Answers](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.32.3.16 **Questions- 103.16.1 -Granting & Removing Access to Generic Account - Option 1 Sites**

28. Which of the following is an **ACCURATE** statement?
- a. “Generic” CCIS accounts were established to serve as the primary address for the CCIS to receive official communication from OCDEL as well as inquiries from Internet users with questions about the COMPASS application process.
  - b. The “Generic” address is attached to an office or location.
  - c. Access to the e-mail account may be granted through the “Permissions” function in Microsoft Outlook.
  - d. All of the above.

[Return to Table of Contents](#)

[Return to Manual Section “103.16.1 - Granting & Removing Access to Generic Account - Option 1 Sites”](#)

[See Answers](#)

## 103.32.3.17 **Questions- 103.16.4 -Account Passwords - All Sites**

29. TRUE or FALSE. You may give your password to a co-worker when you are going on vacation and that co-worker is covering your caseload while you are away.

[Return to Table of Contents](#)

[Return to Manual Section “103.16.4 - Account Passwords - All Sites”](#)

[See Answers](#)

## **103.32.3.18 Questions- 103.16.4.1 -Creating Passwords**

30. When creating passwords for the generic account, the CCIS must ensure the password meets which of the following requirements?
- a. Be at least seven (7) characters in length.
  - b. Not contain the name or birthdates of an individual in your family or a family pet.
  - c. Contain characters from at least three (3) of the following categories:
    - i. Upper case letters.
    - ii. Lower case letters.
    - iii. Numbers.
    - iv. Special characters, such as \*, @, #.
  - d. (a) and (c) above.
  - e. All of the above.

[Return to Table of Contents](#)

[Return to Manual Section "103.16.4.1 -Creating Passwords"](#)

[See Answers](#)

## **103.32.3.19 Questions- 103.16.4.2 - Changing Passwords**

31. TRUE or FALSE. The password must be changed every 60 days.
32. TRUE or FALSE. Once used, a password cannot be re-used for 6 cycles.

[Return to Table of Contents](#)

[Return to Manual Section "103.16.4.2 -Changing Passwords"](#)

[See Answers](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.32.3.20 Questions- 103.16.4.3 - Lock-outs

33. A user will be locked-out after how many consecutive invalid log-on attempts? \_\_\_\_\_

34. Under what circumstances is a log-on attempt considered invalid?

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

[Return to Table of Contents](#)

[Return to Manual Section "103.16.4.3 -Lock-outs"](#)

[See Answers](#)

## 103.32.3.21 Questions- 103.20 -Family File & Subpoenas

35. List the basic guidelines to follow when establishing and maintaining a family file.

a. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

b. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

c. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

# GENERAL OPERATIONAL INFORMATION

---

d. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

e. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

f. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

g. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

36. TRUE or FALSE. Any member of the family or authorized person acting on behalf of the family, including advocates or legal representatives, may review the family file during the CCIS agency's regular operating hours.

37. TRUE or FALSE. When presented with a subpoena, the CCIS may release information about the p/c and/or the p/c's children.

38. What must the CCIS do when presented with a subpoena?  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

[Return to Table of Contents](#)

[Return to Manual Section "103.20 – Family File & Subpoenas"](#)

[See Answers](#)



## **103.32.3.22 Questions- 103.21 -Record Retention**

39. The CCIS shall retain family files for at least \_\_\_\_ years from the end of the fiscal year in which subsidized child care has been provided or until an audit or litigation is resolved.

[Return to Table of Contents](#)

[Return to Manual Section "103.21 - Record Retention"](#)

[See Answers](#)

## **103.32.3.23 Questions- 103.22 -Reporting Child Abuse**

40. TRUE or FALSE. The CCIS is a mandated reporter and must report all suspected child abuse.

[Return to Table of Contents](#)

[Return to Manual Section "103.22 - Reporting Child Abuse"](#)

[See Answers](#)

## **103.32.3.24 Questions- 103.23 -Provider Complaints**

41. TRUE or FALSE. The CCIS may not report a complaint about a child day care facility to the Regional OCDEL Office on behalf of a p/c.

[Return to Table of Contents](#)

[Return to Manual Section "103.23 - Provider Complaints"](#)

[See Answers](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.32.3.25 Questions- 103.24.1 -PA Key, Regional Key

42. Collaboration with the PA Key includes:

a. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

b. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

c. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

d. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

[Return to Table of Contents](#)

[Return to Manual Section "103.24.1 - PA Key"](#)

[See Answers](#)

## 103.32.3.26 Questions- 103.24.3 -E&T Contractors

43. TRUE or FALSE. The CCIS must submit *Form 1540 - Quarterly Employment Report* on a quarterly basis.

[Return to Table of Contents](#)

[Return to Manual Section "103.24.3 - E&T Contractors"](#)

[See Answers](#)

# GENERAL OPERATIONAL INFORMATION

---

## **103.32.3.27 Questions- 103.24.4 -Regional OCDEL Offices**

44. What must the CCIS do when it discovers a critical provider payment issue?

---

---

---

---

---

[Return to Table of Contents](#)

[Return to Manual Section "103.24.4 - Regional OCDEL Offices"](#)

[See Answers](#)

## **103.32.3.28 Questions- 103.24.5 -IRS**

45. TRUE or FALSE. The CCIS must share information on the EITC with families participating in the subsidized child care program.

[Return to Table of Contents](#)

[Return to Manual Section "103.24.5 - IRS"](#)

[See Answers](#)

## **103.32.3.29 Questions- 103.24.7 -OCYF & Sharing Information regarding Keystone STARS Placement**

46. TRUE or FALSE. CCIS agencies must provide their local CYS with provider rate information and lists of STARS 2 and above providers.

[Return to Table of Contents](#)

[Return to Manual Section "103.24.7 - Help Desk"](#)

[See Answers](#)

# GENERAL OPERATIONAL INFORMATION

---

## **103.32.3.30 Questions- 103.25 -HELPLINE**

47. What must the CCIS have to do to ensure an effective working relationship with the HELPLINE?

a. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

b. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

[Return to Table of Contents](#)

[Return to Manual Section "103.25 - HELPLINE"](#)

[See Answers](#)

## **103.32.3.31 Questions- 103.26 -Help Desk**

48. TRUE or FALSE. The CCIS may contact the Help Desk for policy clarification and/or system-related problems.

[Return to Table of Contents](#)

[Return to Manual Section "103.26 - Help Desk"](#)

[See Answers](#)

## **103.32.3.32 Questions- 103.27 -Staffing, Training Needs & Coordination**

49. TRUE or FALSE. The CCIS is required to employ individuals receiving public assistance from the Department and to submit quarterly reports of hiring under the CCIS plan for recruiting and hiring public assistance recipients.

# GENERAL OPERATIONAL INFORMATION

---

50. List the criteria that apply to staff training.

a. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

b. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

c. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

d. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

[Return to Table of Contents](#)

[Return to Manual Section "103.27 - Staffing, Training Needs & Coordination"](#)

[See Answers](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.32.4 Section Checkpoint Answers

The Policy and Operations Divisions of the Bureau of Subsidized Child Care Services provided the answers to all of the questions asked in Manual Section “413.24.3 – Section Checkpoint Questions”.

### 103.32.4.1 Answers – 103.5 – Subsidized Child Care Program Objectives

1. The Department’s overall objectives for the subsidized child care program include:
  - a. Assist in the payment of child care services for eligible families whose children need child care while the p/c is working or meeting the CAO E&T requirements, completing high school or participating in training while working a minimum of ten hours per week.
  - b. Provide parent education regarding the benefits of quality child care.
  - c. Provide R&R services free of charge to all families whether or not they qualify for subsidized child care.
  - d. Assure that an eligible family is able to choose a child care setting that is appropriate for the child(ren) in the family including licensed, registered and R/N child care providers.
  - e. Allow a legally-operating child care provider the opportunity to participate in the subsidized child care program.
  - f. Distribute funds in a manner that maximizes the service funding available for subsidized child care.

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section “103.5 – Subsidized Child Care Program Objectives”](#)

[Proceed to Manual Section “103.6 – Contact Information”](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.32.4.2 Answers - 103.9 - Public Access

2. **TRUE**. The CCIS must be open for business and physically present to answer subsidized child care questions from the general public between the hours of 8:30 a.m. and 5:00 p.m., Monday through Friday, except on state-recognized holidays or in the case of County Government managed programs, county-recognized holidays.
3. **FALSE**. The CCIS must be accessible to a p/c and/or provider who cannot contact the agency during the weekday office hours, but is not required to establish weekend hours.
4. **NO**. The toll-free telephone line may not have voice-mail as the primary mechanism for handling incoming telephone calls between the hours of 8:30 a.m. and 5:00 p.m., Monday through Friday, except on state-recognized holidays or in the case of County Government managed programs, county-recognized holidays?
5. The CCIS must ensure that each of its staff responds to voice-mail messages within **two (2)** working days.

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.9 - Public Access"](#)

[Proceed to Manual Section "103.10 - Nondiscrimination"](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.32.4.3 Answers - 103.11 - Confidentiality

6. The CCIS must take additional steps to further safeguard information when any of the following are true:
  - a. Teen parent cases in which the teen parent is 13 years of age or younger.
  - b. CCIS employee.
  - c. Domestic or other violence.

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.11 - Confidentiality"](#)

[Proceed to Manual Section "103.12 - HIPAA"](#)

## 103.32.4.4 Answers - 103.12 - HIPAA

7. e. - (a) through (c) only.  
Protected Health Information (PHI) may be disclosed under the following circumstances:
  - a. When the Privacy Rule permits or requires.
  - b. When the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.
  - c. When Health and Human Services (HHS) is undertaking a compliance investigation, review or enforcement action.

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.12 - HIPAA"](#)

[Proceed to Manual Section "103.13 - LEP"](#)



# GENERAL OPERATIONAL INFORMATION

---

## 103.32.4.5 Answers - 103.13 - LEP

8. **The CCIS may contract with the LanguageLine or any other equivalent service provider, in order to assist in working with persons with LEP.**
9. **g. - All of the above.** The following are examples of practices that may violate Title VI with regard to LEP:
  - Providing services that are more limited in scope or are lower in quality.
  - Unreasonable delays in the delivery of services.
  - Limiting participation in a program or activity.
  - Providing services that are not as effective.
  - Failing to inform a person of the right to receive free interpreter services.
  - Requiring a person to provide his own interpreter.
10. **The type of language assistance the CCIS provides will depends upon the CCIS size, the size of the eligible LEP population, the total resources available to the CCIS, the frequency with which particular languages are encountered and the frequency with which persons with LEP come into contact with the CCIS.**

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.13 - LEP"](#)

[Proceed to Manual Section "103.14 - Acceptable Use of IT Resources"](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.32.4.6 Answers - 103.14 - Acceptable Use of IT Resources

11. The following are examples of Commonwealth IT resources:
  - a. *The Commonwealth's computer systems, together with any electronic resource used for communications, which includes, but is not limited to laptops and individual desktop computers.*
  - b. *Wired or wireless telephones, cellular phones, pagers, beepers, personal data assistants and handheld devices (i.e., a Blackberry device, Palm devices, etc., and, further, includes use of the Internet, e-mail.*
  - c. *Instant messaging, texting, voice mail, facsimile, copiers, printers or other electronic messaging through Commonwealth facilities, equipment or networks.*

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.14 - Acceptable Use of IT Resources"](#)

[Proceed to Manual Section "103.14.1 - General Policy"](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.32.4.7 Answers- 103.14.2.2 - Expectation of Privacy - Internet

12. **TRUE.** All user activity involving internet use is subject to tracking, blocking, logging, auditing, monitoring, accessing, retrieving and reviewing by the Department. All data and records, including those pertaining to computer use, Internet use, e-mail communication, voicemail communication, text messages and other electronic communication (whether sent, received, or stored), as well as the content of such communications, are presumed to be the sole and exclusive property of the Commonwealth. Individual Authorized Users do not control the access to or the use of such data or records. In addition, Authorized Users have no property or other rights to any or all related physical equipment, hardware and software applications that are provided, stored or otherwise utilized in connection with IT Resources.

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section “103.14.2.2 - Expectation of Privacy - Internet”](#)

[Proceed to Manual Section “103.14.2.3 - Access & Authorization - Internet”](#)

## 103.32.4.8 Answers - 103.14.3.1 - Expectation of Privacy - E-mail

13. **When sensitive material is sent electronically via e-mail, it is important to verify that all recipients are authorized to receive such information and to understand that e-mail is not fully secure and/or private, except where appropriate security applications are used (i.e., data encryption).**

# GENERAL OPERATIONAL INFORMATION

---

14. *When it is necessary to transmit Commonwealth proprietary or restricted information beyond the Commonwealth Connect e-mail network, the messages must be protected by encryption.*

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.14.3.1 – Expectation of Privacy – E-mail"](#)

[Proceed to Manual Section "103.14.3.2 – Access & Authorization – Email"](#)

## 103.32.4.9 Answers – 103.14.3.4 – Security Issues

15. *A CCIS user secures his/her desktop by pressing "Ctrl" and "Alt" and "Delete" on the keyboard, then select "Lock Computer".*

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.14.3.4 – Security Issues"](#)

[Proceed to Manual Section "103.14.3.5 – Acceptable Use – E-mail"](#)

## 103.32.4.10 Answers – 103.14.3.6 – Encryption

16. *An email must be encrypted if the user is sending it to a recipient outside the Commonwealth system AND it contains sensitive information.* Sensitive information includes Social Security numbers; financial data; personal health information; legal documents; personnel information; and/or general personal information.

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.14.3.6 – Encryption"](#)

[Proceed to Manual Section "103.14.4 – Unacceptable Use of IT Resources"](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.32.4.11 Answers - 103.14.4 - Unacceptable Use of IT Resources

17. YES.
18. Jim shared his username and password with Ted. You may not share your username or password. Also, Jim had his username and password on a sticky note posted on his computer. Do not write your username or password down and do not store the information near your computer.
19. YES.
20. Toni opened an e-mail and an attachment from an unknown sender. If you can avoid it, do not open e-mail from senders you do not recognize. Delete the e-mail. Even if you recognize the sender, if the contents seem out-of-character or questionable, delete the e-mail. Never click on links, open attachments or download anything unless you are 100% sure it is safe. Also, Toni gave the sender sensitive and personal information. Never respond to e-mails that ask for sensitive or personally identifiable information, like usernames, passwords, employee ID numbers, bank account or credit card numbers, etc. Never enter sensitive information into a web page/form that you access by clicking on a link in an e-mail or into an automated telephone system if the telephone number was provided in the e-mail.
21. YES.

# GENERAL OPERATIONAL INFORMATION

---

22. **Stacy left her mobile device unsecured on the front seat of her car. It's best to keep your mobile devices, such as laptops, BlackBerries, cell phones and similar items with you. If these items are not with you, the items should be locked up safely. Never leave your mobile devices unattended, unsecured or visible in places like your office/cubicle/work area, a meeting room, the bathroom, in the console of your car or on a car seat. In addition, Stacy did not immediately report her lost mobile device. If your mobile device is lost for even a short period of time or damaged in any way, it is critical that you contact your agency's IT office/department or administrator immediately. Do not delay for any reason.**

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.14.4 – Unacceptable Use of IT Resources"](#)

[Proceed to Manual Section "103.14.5 – Data Cleansing & Disposal of IT Resources"](#)

## 103.32.4.12 **Answers – 103.14.5 – Data Cleansing & Disposal of IT Resources**

23. **TRUE.** Peripheral storage devices including but not limited to floppy diskettes, CD and DVD discs along with external storage devices such as USB drives, may be used by end users for storing Commonwealth data when the user is directed to do so by his/her agency's IT staff or administrator.

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.14.5 – Data Cleansing & Disposal of IT Resources"](#)

[Proceed to Manual Section "103.14.6 – Desktop & Server Software Patches"](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.32.4.13 Answers - 103.14.6 -Desktop & Server Software Patches

24. *At the end of the day the user must make sure all computers or tablets are logged off with power left on, including over the week-end, in order to receive the security patches that will be sent out.*

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.14.6 - Desktop & Server Software Patches"](#)

[Proceed to Manual Section "103.14.6.1- Unsupported Software"](#)

## 103.32.4.14 Answers - 103.15 - CIS Passwords

25. *b. - 6 months.* CIS passwords expire 6 months from the date the user changes his/her password.
26. *OCDEL recommends that CCIS staff log-on to CIS at least once a month, even if there is not an immediate business need to do so, to prevent users from being locked-out of CIS.*

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.15- CIS Passwords"](#)

[Proceed to Manual Section "103.16- Department E-mail Accounts"](#)

## 103.32.4.15 Answers - 103.16 -Department E-mail Accounts

27. *c. - There is no difference between Option 1 and Option 2 sites when accessing CWOPA.*

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.16- Department E-mail Accounts"](#)

[Proceed to Manual Section "103.16.1 - Granting & Removing Access to Generic Account - Option 1 Sites"](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.32.4.16 Answers - 103.16.1 -Granting & Removing Access to Generic Account - Option 1 Sites

28. d. - All of the above.

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.16.1 - Granting & Removing Access to Generic Account - Option 1 Sites"](#)

[Proceed to Manual Section "103.16.2- Granting & Removing Access to R&R Account - Option 1 Sites"](#)

## 103.32.4.17 Answers - 103.16.4 -Account Passwords - All Sites

29. FALSE. You may NOT give your password to a co-worker when you are going on vacation and that co-worker is covering your caseload while you are away.

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.16.4- Account Passwords - All Sites"](#)

[Proceed to Manual Section "103.16.4.1 - Creating Passwords"](#)

## 103.32.4.18 Answers - 103.16.4.1 -Creating Passwords

30. d. - (a) and (c) above. There is no requirement regarding the use of family member's or pet's names or birthdates as a portion of your password.

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.16.4.1 - Creating Passwords"](#)

[Proceed to Manual Section "103.16.4.2- Changing Passwords"](#)



# GENERAL OPERATIONAL INFORMATION

---

## 103.32.4.19 Answers - 103.16.4.2 - Changing Passwords

31. **TRUE**. The password must be changed every 60 days.
32. **TRUE**. Once used, a password cannot be re-used for 6 cycles.

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.16.4.2 - Changing Passwords"](#)

[Proceed to Manual Section "103.16.4.3 - Lock-outs"](#)

## 103.32.4.20 Answers - 103.16.4.3 - Lock-outs

33. A user will be locked-out after ***five (5)*** consecutive invalid log-on attempts.
34. ***The following are considered invalid log-on attempts: if the username and password are not entered exactly as established or if the "Num Lock" key is not "on".***

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.16.4.3 - Lock-outs"](#)

[Proceed to Manual Section "103.17- Political Activity Guidelines"](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.32.4.21 Answers - 103.20 - Family File & Subpoenas

35. The following are basic guidelines to follow when establishing and maintaining a family file:
- a. **Only one case file is necessary.**
  - b. **Maintain the most current information on the top of the file.**
  - c. **All information documenting a specific application or redetermination must be kept together in a systematic manner so each eligibility period is separate and easily identified.**
  - d. **Breaks in eligibility segments should be apparent.**
  - e. **File "one time only" information with the current application or in a specific section of the file folder.**
  - f. **Mark documentation that is used to verify multiple eligibility segments so it is easily located.**
  - g. **There is no need to keep case comments in the family file unless the comments are related to special circumstances.**
36. **TRUE.** Any member of the family or authorized person acting on behalf of the family, including advocates or legal representatives, may review the family file during the CCIS's regular operating hours.
37. **FALSE.** When presented with a subpoena, the CCIS may **NOT** release information about the p/c and/or the p/c's children.
38. **When presented with a subpoena, the CCIS should respond in writing using the CCIS Response to Subpoena document.**

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.20- Family File & Subpoenas"](#)

[Proceed to Manual Section "103.21 - Record Retention"](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.32.4.22 Answers - 103.21 -Record Retention

39. The CCIS shall retain family files for at least ***six (6)*** years from the end of the fiscal year in which subsidized child care has been provided or until an audit or litigation is resolved.

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.21 - Record Retention"](#)

[Proceed to Manual Section "103.22- Reporting Child Abuse"](#)

## 103.32.4.23 Answers - 103.22 -Reporting Child Abuse

40. ***TRUE***. The CCIS is a mandated reporter and must report all suspected child abuse.

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.22- Reporting Child Abuse"](#)

[Proceed to Manual Section "103.23 - Provider Complaints"](#)

## 103.32.4.24 Answers - 103.23 -Provider Complaints

41. ***FALSE***. Although the CCIS should encourage the p/c to report a complaint about a child day care facility to the Regional OCDEL Office directly, the CCIS may report a complaint on behalf of a p/c if the p/c fails to report a complaint.

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.23 - Provider Complaints"](#)

[Proceed to Manual Section "103.24- Working with other Agencies"](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.32.4.25 Answers - 103.24.1 -PA Key

42. Collaboration with the PA Key includes:
- a. *Participating as a hub to promote widespread parental knowledge of Keystone STARS. This work involves cooperation and proactive coordination with the Regional Keys.*
  - b. *Working proactively with groups that support the Keys to promote early learning services that will benefit children and families in their community.*
  - c. *Identifying p/c and provider information needed to complete community needs assessments which is available at CCIS agencies through reports generated from PELICAN CCW.*
  - d. *Keeping informed of public education activities and events.*

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.24.1 - PA Key"](#)

[Proceed to Manual Section "103.24.2-CAO"](#)

## 103.32.4.26 Answers - 103.24.3 -E&T Contractors

43. *TRUE.* The CCIS must submit *Form 1540 - Quarterly Employment Report* on a quarterly basis.

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.24.3 - E&T Contractors"](#)

[Proceed to Manual Section "103.24.4-Regional OCDEL Offices"](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.32.4.27 Answers - 103.24.4 -Regional OCDEL Offices

44. *The CCIS first contacts the Subsidy Coordinator to explain the issue. The Subsidy Coordinator will discuss the issue with regional Certification staff to try to resolve the issue. If the Subsidy Coordinator cannot solve the concern easily, the CCIS then calls the Help Desk so a PCR can be entered to address the problem.*

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.24.4-Regional OCDEL Offices"](#)

[Proceed to Manual Section "103.24.5 - IRS"](#)

## 103.32.4.28 Answers - 103.24.5 -IRS

45. *TRUE.* The CCIS must share information on the EITC with families participating in the subsidized child care program.

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.24.5 - IRS"](#)

[Proceed to Manual Section "103.24.6-OIG"](#)

## 103.32.4.29 Answers - 103.24.7 - OCYF & Sharing Information regarding Keystone STARS Placements

46. *TRUE.* CCIS agencies must provide their local CYS with provider rate information and lists of STAR 2 and above providers.

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.24.7 - OCYF & Sharing Information regarding Keystone STARS Placements"](#)

[Proceed to Manual Section "103.25-HELPLINE"](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.32.4.30 Answers - 103.25 -HELPLINE

47. The CCIS must do the following to ensure an effective working relationship with the HELPLINE:
- a. Designate a “contact person” for calls from the HELPLINE.
  - b. Attempt to resolve the issue with the p/c and then contact the HELPLINE to confirm how the issue was resolved.

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section “103.25 – HELPLINE”](#)

[Proceed to Manual Section “103.26 – Help Desk”](#)

## 103.32.4.31 Answers - 103.26 -Help Desk

48. **FALSE.** The CCIS may contact the Help Desk for system-related issues only. The CCIS should continue to direct questions or issues related to policy to the assigned Subsidy Coordinator. The Subsidy Coordinator continues to be the “first line of defense” for the CCIS for these and other non-system issues.

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section “103.26 -Help Desk”](#)

[Proceed to Manual Section “103.27 – Staffing, Training Needs & Coordination”](#)

# GENERAL OPERATIONAL INFORMATION

---

## 103.32.4.32 **Answers - 103.27 -Staffing, Training Needs & Coordination**

49. **TRUE.** The CCIS is required to employ individuals receiving public assistance from the Department and to submit quarterly reports of hiring under the CCIS plan for recruiting and hiring public assistance recipients.
50. The following criteria apply to staff training:
- a. **New staff must be trained within 60 calendar days of their start date for all aspects of their job assignments.**
  - b. **Staff must receive ongoing training within 30 calendar days of updates or changes to any aspect of their job assignments.**
  - c. **Staff must be cross-trained to assure that core functions are able to be performed in the event of staff vacancies and/or absences.**
  - d. **A training plan must be established by each CCIS.**

[Return to Table of Contents](#)

[Review Questions Again](#)

[Return to Manual Section "103.27 - Staffing, Training Needs & Coordination"](#)

[Proceed to Manual Section "103.28 - OCDEL Responsibilities"](#)