



Policy and Procedure Manual

Volume 2, Chapter 8 Electronic Devices, Security and Service Interruption Plan

Washington State WIC Nutrition Program

DOH 960-368

Effective June 15, 2022



This institution is an equal opportunity provider.

Washington WIC doesn't discriminate.

For persons with disabilities, this document is available on request in other formats.

To submit a request, please call 1-800-841-1410 (TDD/TTY 1-800-833-6388).

PUBLIC HEALTH
ALWAYS WORKING FOR A SAFER AND
HEALTHIER WASHINGTON



Electronic Devices, Security and Service Interruption Plan

Section 1: Definitions	1
Definitions:.....	1
Section 2: Locations and Electronic Devices for Providing WIC Services	2
POLICY: Provide WIC Services at State Approved Clinics Only.....	2
POLICY: Electronic Devices to Provide WIC Services.....	3
POLICY: Cell Phones	5
POLICY: Internet Use	8
POLICY: Order Printer Cartridges.....	9
Section 3: Security	10
POLICY: Physical Security and Care of State Owned Electronic Devices	10
POLICY: Assure Security of Software and Data	12
POLICY: Breach in Security due to Lost or Stolen Electronic Devices.....	13
POLICY: Staff Access to Software and Data	14
POLICY: Use a Secure Network to Access Cascades.....	16
POLICY: Secure Access Washington (SAW) Account	17
POLICY: Passwords	18
Section 4: Support	19
POLICY: Support for State Owned Electronic Devices.....	19
POLICY: Support for Cascades Software	20
Section 5: Service Interruption Plan	21
POLICY: WIC Services when Cascades is Unavailable.....	21

POLICY: Electronic Benefit Transfer (EBT) Provider is Unavailable 23

Section 6: Appendix 25

EXAMPLE: Cellular Device Authorization and Agreement 26

Service Interruption Action Plan..... 28

Section 1: Definitions

Definitions:

1. **Cascades Support:** State WIC staff who support the Cascades application.
2. **Electronic Devices/Hardware:** Physical and mechanical components of computers, such as the desktop, laptop, monitor, keyboard, mouse, printers, modem, switches, cabling, and cell phones.
3. **HTS Service Desk:** Department of Health staff in the Health Technology Solutions unit, who support the WIC state owned electronic devices used in local WIC agencies.
4. **Software:** Applications installed on the electronic device.
5. **Local Agency Owned:** Electronic devices purchased with local agency funds supported and managed by local IT.
6. **Local IT:** Staff in the local agency who handle the agency's Information Technology (IT) needs and support agency owned electronic devices.
7. **Peripherals:** Includes the scanner, card reader, and signature pad.
8. **State Owned:** Electronic devices loaned by Washington WIC to the local agency and supported and managed by the HTS Service Desk.

Section 2: Locations and Electronic Devices for Providing WIC Services

POLICY: Provide WIC Services at State Approved Clinics Only

The local agency must:

- Provide WIC services only at state approved clinics.
- Request and receive state approval to provide services at any other locations.

PROCEDURE:

A. The coordinator:

1. Submits a request for a new clinic in writing to the Local Program Consultant (LPC) for review.
 - Sends requests to the LPC mailbox at WICLPC@doh.wa.gov.
2. Waits for approval before conducting services.

B. Staff:

1. Follow all electronic device and data security policies in this chapter.

Information:

All clinics where WIC services are provided are subject to monitoring.

POLICY: Electronic Devices to Provide WIC Services

The coordinator must assure:

- Staff use state owned electronic devices to provide WIC services, or have permission from the Local Program Consultant (LPC) to use agency owned or other devices.
- All computers running the Cascades application meet requirements listed in Procedure below.
- Agency owned electronic devices have local IT support.
 - The local IT support must coordinate with the Health Technology Solutions (HTS) Service Desk on configurations and security requirements.
- BFPC laptop computers remain the property of Department of Health WIC Program.

Note: All information pertaining to WIC business is subject to Public Disclosure. This includes information stored on any electronic devices.

PROCEDURE:

The Coordinator:

- A. Requests state owned electronic devices from the LPC.
 - 1. Send requests to the LPC mailbox at WICLPC@doh.wa.gov.
 - 2. The LPC approves or denies the request.
 - 3. The LPC submits approved requests to HTS.
 - HTS works directly with the coordinator to schedule time for delivery and set up of electronic devices.
- B. Contacts the LPC to use agency owned electronic devices to conduct WIC business.
 - Send requests to the LPC mailbox at WICLPC@doh.wa.gov
- C. Assures computers running the Cascades application meet the following requirements:
 - Has the most current Microsoft security patches.

- Uses a current version of the Windows operating system.
- Has an active virus protection.
- Uses the internet browser(s) specified by HTS, updated with most recent security patches.
- Is encrypted.
- Has installed Net 4.7.1 or newer version.
- The device lock out is set at 10 minutes.
- Has peripherals configured in a way that allows updates for the latest firmware.
- Allows DOH to provide support using GoToAssist.

POLICY: Cell Phones

Staff must:

1. Use cell phones bought with WIC federal funds for WIC purposes only.
2. Assure cost-sharing occurs for cell phones used for more than one program.
3. Use only agency-issued cell phones, not personal cell phones.
4. Submit exception requests to the Local Program Consultant for prior approval.

Cell phones must have:

1. Mobile Device Management (MDM) software that can locate, lock, and wipe a lost device.
2. Login and password protections that meet state agency security requirements. See the [“Passwords”](#) policy in this chapter.

Staff must do the following to use text messaging:

1. Ask for and document participant permission to receive text messages.
 - a. If the participant’s preferred method of contact is texting, staff document their permission to receive texts by indicating Text as the preferred method of contact on the Family Demographics screen.
 - b. If the participant prefers another primary method of contact, but also gives permission to receive texts, staff document on a Sticky Note on the Family Demographics screen.
 - c. If the local agency has a more stringent process, staff follow the more stringent process.
2. Assure participant contact information and text messages on cell phones meet all the requirements of safeguarding participant information.
 - See [Volume 1, Chapter 25, Legal Considerations and Confidentiality](#), Section 5, Safeguarding Client Information.

Text messages are not secure and must not:

1. Include any personal health information.
2. Include any identifiable data such as social security or driver's license numbers.
3. Include photos of proofs or other documents with personal information.

Text messages must:

1. Use only easily understood abbreviations that don't change the meaning of the message.
2. Be limited to:
 - a. Scheduling appointments and appointment reminders.
 - b. Inviting participants to video chats or phone calls.
 - c. Short check-ins, basic information, or confirmation of phone calls or appointments.
 - Use video-chat, phone or in person methods for issues that require more than a simple check-in.
 - d. Sending links to nutrition education materials if the participant has confirmed they want to receive them.
 - Send only links, not the materials themselves, as sending the materials may inadvertently use the participant's phone's data or take up storage space on their device.
 - e. Following up on requested information, if the text contains no sensitive information.
 - f. Sending promotional messages, such as encouraging FMNP check usage, upcoming events.
 - g. Sending emergency messages, such as agency closure.

Note: State monitor staff can review text messages sent on WIC funded cell phones for compliance with this policy.

3. Be documented in the participant's Individual Care Plan when there is a two-way dialogue.
 - a. Do not document "canned" text messages, sending nutrition education links, one way education or encouragement. "Canned" text messages include notifications sent to a group of participants about an event, encouragement, a closure, a reminder, etc.
 - b. Do not document individualized one-way notifications.

Note: Local agencies may choose to document, or not, responses to appointment reminders.

PROCEDURE:

The coordinator:

- A. Complies with the local agency cell phone policy and procedure.
 1. Assure that the local agency cell phone procedures have all the components listed below. If they do not, add an addendum for WIC staff that includes these items.
- B. Develops a cell phone policy and procedure if the local agency doesn't have one. The policy and procedure addresses:
 1. When staff must turn on cell phones and when they should, or may be, turned off.
 - a. Most staff turn on cell phones during business hours.
 - b. Peer counselors turn on cell phone during business hours and additional times as agreed.
 2. Description of a standard greeting for answering the phone and for voice mail.
 3. Response time for returning calls or texts.
- C. Trains and documents cell phone policy and procedure with all new staff and with all staff with cell phones at least annually.
- D. Has the employee sign an "Employee cell phone agreement" and keep on file for four years. See sample [Cellular Device Authorization and Agreement](#) in the Appendix.

POLICY: Internet Use

Internet use on state owned electronic devices is for WIC business only. WIC business includes accessing Cascades, clinic staff work email, and websites used for nutrition research, etc.

Staff must not use state owned electronic devices to access the internet for personal use. Examples include personal email, social media, school, etc.

If there's a question regarding a specific website used for WIC business, staff must request clarification and approval from the Local Program Consultant (LPC) prior to accessing the website.

Note: The Health Technology Solutions (HTS) Service Desk randomly reviews internet use on state owned electronic devices when issues arise such as viruses and/or at the request of a coordinator. If staff visit or access questionable sites, HTS notifies the Coordinator for follow-up.

Follow local agency internet policy if more restrictive than state WIC policy.

PROCEDURE:

Staff:

- A. Only use the internet on state owned electronic devices for WIC business.
- B. Ask for clarification from the Local Program Consultant (LPC) when there are questions about specific websites for WIC business use.
 1. If clinic staff want to access social media sites for outreach purposes, request approval from the LPC.
 2. The LPC notifies staff in writing when access is approved.

Note: Staff don't have to request permission to access sites such as USDA, Journal of the American Medical Association (JAMA), Academy of Nutrition and Dietetics (AND), and Nutrition First.

POLICY: Order Printer Cartridges

The Coordinator, or designated clinic staff order printer cartridges through the state WIC Program.

Order no more than one extra printer cartridge at a time for each state owned printer.

PROCEDURE:

Staff:

- A. Order a new cartridge when replacing a cartridge in the printer.
 - 1. Do not stockpile cartridges.
- B. Complete the printer cartridge order form located on the [Program Forms and Materials](#), and follow instructions on the form to submit to the state office.

Section 3: Security

POLICY: Physical Security and Care of State Owned Electronic Devices

Staff must assure the physical security and care of state owned electronic devices. This includes:

- Provide reasonable protection from theft or loss.
- Take security measures at clinics and while in transit between clinics.
- Take care of electronic devices to prevent damage.

Local agencies must:

1. Have written procedures to assure the physical security of state owned electronic devices.
2. Provide in-service training on these procedures to staff each year and document on the staff training log.

PROCEDURE:

Staff:

- A. Lock the clinic or areas of the clinic where electronic devices containing participant and staff data are stored when not in use.
- B. Store moveable items, including cell phones, in locked cabinets when not in use.
- C. Use anti-theft devices, like cable tie-downs, to secure hardware and other electronic devices to desks and tables.
- D. Retrieve building keys or access badges when employees leave employment.
- E. Change door locks when electronic devices have been stolen.
- F. Consider a security system in areas of high theft.
- G. Use appropriate carrying cases that protect portable electronic devices during transport.
- H. When transporting electronic devices in a vehicle, keep them out of sight and lock the vehicle when unoccupied.

1. Remove electronic devices from vehicles when not in transit for long durations such as overnight or over the weekend.
 2. Don't leave electronic devices in a vehicle during extreme hot or cold weather.
- I. Prevent damage to electronic devices.
1. Don't place anything on top of electronic devices.
 2. Keep devices within acceptable temperature ranges (35-85 degrees Fahrenheit).
 3. Use surge protectors between electronic devices and electrical outlets.
 - a. Only plug the electronic devices into the surge protector. Don't plug additional items into the same surge protector (i.e. radios, fans, heaters, etc.).
 4. Take precautions to prevent damage from natural disasters. While staff should protect all state owned electronic devices, here are special precautions for state owned computer devices. Notify the HTS Service Desk if any of the following occur:
 - a. Power Outages: Close all files when power flickers, turn off the hardware and pull the surge protector plug out of the electrical outlet.
 - b. Flooding: Protect hardware from water damage by storing in a secure, dry place. Move electrical cords and surge protectors to dry locations when there's a risk for flooding or you have a reason to expect water damage in the work area.
 - c. Fire: Protect hardware from fire damage by keeping flammable material away from power outlets and surge protectors. Don't overload outlets or surge protectors by attaching multiple outlet splitters or surge protectors in a chain.
 - d. Earthquake: Don't place hardware any higher than desk level.

POLICY: Assure Security of Software and Data

Staff must take precautions to assure the security and integrity of software and data containing participant and staff information on state and agency owned electronic devices.

Notes:

- Staff may store personnel files on an agency thumb drive or external hard drive and access them on state owned computers, **as long as the files aren't stored on the state-owned computer.**
- State WIC staff can access state owned computers to secure participant information and track the computer if it's lost or stolen.
- State staff can't access agency owned computers in this way, so participant information can't be saved to the local agency computer outside of the Cascades application.

PROCEDURE:

Staff:

- A. Lock the clinic or areas of the clinic where electronic devices containing participant and staff data are stored when not in use.
 - See the "[Physical Security of State Owned Electronic Devices](#)" policy in this chapter and [Volume 1, Chapter 25 - Legal Considerations and Confidentiality](#).
- B. Lock the electronic device when stepping away from the desk or the device.
- C. Follow the requirements in the "[Passwords](#)" policy.
- D. Receive annual training on confidentiality.
 - The confidentiality training and policy contains information about not storing personnel or personal information on state owned electronic devices.
 - See the policy "Assure Client Confidentiality at the Time of Providing Services" in [Volume 1, Chapter 25 – Legal Consideration and Confidentiality](#).

POLICY: Breach in Security due to Lost or Stolen Electronic Devices

The coordinator must:

- Notify the Local Program Consultant (LPC) within 1 business day of discovering a potential breach in security due to lost or stolen electronic devices.
- Work with the LPC on a plan for notifying participants about the breach in security if participant information was on the device(s).
 - See [Volume 1, Chapter 25 – Legal Considerations and Confidentiality](#) for more information.
- Report to the LPC how staff plan to correct the situation which allowed electronic devices to be lost or stolen.

Note: See [Volume 2, Chapter 5 – Purchasing and Inventory](#) for information about reporting lost, stolen or destroyed electronic devices.

PROCEDURE:

The coordinator:

- A. Notifies the LPC about lost or stolen electronic devices and works on a notification plan if participant information was on the devices.
 - Call 1-800-841-1410 and ask for the LPC, or send an email to WICLPC@doh.wa.gov.

POLICY: Staff Access to Software and Data

The coordinator must assure the security and integrity of software and data by activating or inactivating staff access as appropriate.

PROCEDURE:

The coordinator:

- A. Activates or reactivates access to Windows and Cascades for employees.
 1. Send a request to the HTS Service Desk for a temporary Windows log on.
 2. Contact HTS at: wic.helpdesk@doh.wa.gov
 - Notifies the local IT staff to disable Windows if network access is through the local agency network.
 3. Activates staff access to Cascades.
 - See the “[Secure Access Washington](#)” policy for more information.
- B. Inactivates access to Windows and Cascades when an employee is terminated.
 1. Notifies the Health Technology Solutions (HTS) Service Desk to inactivate access to Windows when an employee has been terminated
 - Send staff person’s name, clinic(s) they have access to, and their termination date to wic.helpdesk@doh.wa.gov.
 2. Notifies the local IT staff to disable Windows if network access is through the local agency network.
 3. Inactivates staff access to Cascades.
 - Inactivate staff user ID’s when an employee is terminated or there is a prolonged absence (for example, maternity leave, surgery, etc.).
 - We don’t recommend archiving staff in Cascades because they can’t be reactivated at any time.
- C. Requires new passwords for all staff when there is a security breach that compromises software security.

1. At a minimum staff change their Secure Access Washington (SAW) password.
 2. We recommend staff change their Windows password also.
 - See [Volume 1, Chapter 25 - Legal Considerations and Confidentiality](#) chapter.
- D. Requests approval from the Local Program Consultant (LPC) before allowing non-WIC staff to use state owned electronic devices. Examples include a registered dietitian contractor, auditor, etc.
- Keep documentation of permission from the LPC on file for four years.

POLICY: Use a Secure Network to Access Cascades

Staff must use a secure network to log in to Cascades. Acceptable internet connections include:

- Wired internet connection
- Clinic Wi-Fi
- Password protected Wi-Fi connection
- DOH or local agency issued hot spot or Mi-Fi Connection

Staff must not use public Wi-Fi to access Cascades.

Information:

Contact Health Technology Solutions (HTS) Service Desk at wic.helpdesk@doh.wa.gov or your local IT for questions or assistance.

POLICY: Secure Access Washington (SAW) Account

All staff must have a Secure Access Washington (SAW) account to log in to Cascades.

PROCEDURE:

- A. The coordinator follows instructions for staff SAW accounts located on the [Coordinator's Corner](#) and [Cascades Support](#) webpages.
 - The Coordinator reviews and follows the [Coordinator's Instructions](#).
 - Staff receive an email with directions to create a SAW account.

- B. Staff follow instructions for setting up a SAW account for Cascades production.
 - See [SAW – Handout B SAW for Cascades Production](#).
 - Complete Cascades registration to launch Cascades.

- C. Staff follow instructions for setting up an account for the Cascades Sandbox.
 - See [TEST SAW – Handout 2 Test SAW for Cascades Sandbox](#).

POLICY: Passwords

Staff must use the following password criteria on electronic devices and software used for conducting WIC business:

1. Create a unique password which contains the following:
 - a. At least eight characters.
 - b. A combination of 3 of the following: uppercase letters, lowercase letters, numbers, and special characters or symbols.
2. Create a password that doesn't contain any form of the user's name or their user ID.
3. Never share passwords and don't let another user log on with your account and password.
4. Never use your password to log onto more than one computer at a time.
5. Change passwords every 90 days.
 - Don't use any of the 4 previous passwords.

PROCEDURE:

Staff:

- A. Create their own unique password.
 - We don't recommend using the feature "Remember my password."
- B. Follow all other policy requirements above.

Section 4: Support

POLICY: Support for State Owned Electronic Devices

Staff must contact the Health Technology Solutions (HTS) Service Desk to get support for state owned electronic devices.

PROCEDURE:

Staff:

- A. Follow their agency's protocol for reporting a problem to the HTS Service Desk at 1-888-457-2467.
- B. Work with the HTS Service Desk to get the support needed.

Note: The HTS Service Desk will determine who will resolve issues and arrange for contractor assistance when needed.

POLICY: Support for Cascades Software

Staff must contact Cascades Support for issues with the Cascades software.

- Phone: 1-800-841-1410, option 3, then option 2.
- Email: Cascades.Support@doh.wa.gov

Cascades Support consists of state WIC staff who assist clinic staff using the Cascades application.

PROCEDURE:

Staff:

- A. Follow agency protocol for reporting a problem with Cascades.
- B. Be prepared to provide the following information to Cascades Support staff:
 - Clinic ID
 - Family ID
 - Participant ID
 - Steps leading up to the issue
 - Screenshots as needed
- C. Use the Cascades Support email, Cascades.Support@doh.wa.gov, for non-urgent matters.

Section 5: Service Interruption Plan

POLICY: WIC Services when Cascades is Unavailable

Staff must:

- Provide WIC services when Cascades is unavailable, **and it is safe and appropriate for staff and participants.**

Note: Cascades may be unavailable due to computer failure, software or application problems, internet connectivity issues, power outages or natural disasters.

- Follow the [Guidelines for Using the Cascades WIC Services Worksheets](#) and use the [Pregnant](#), [Breastfeeding/Non-Breastfeeding](#), [Infant](#), and [Child](#) worksheets to gather information from the participant, Parent/Guardian, or Caretaker.

PROCEDURE:

Staff:

- A. Follow the agency's procedures to determine if it is safe and appropriate to provide services to participants.
- B. Contact Cascades Support, HTS Service Desk, or local IT for assistance as needed.
 1. Cascades Support:
 - Call 1-800-841-1410, option 3, then option 2.
 - Email Cascades.Support@doh.wa.gov.
 2. HTS Service Desk:
 - Call: 1-888-457-2467
 - Email DOH_PCH_WIC_Service_Desk@doh.wa.gov
- C. Follow the Guidelines for Using the [Guidelines for Using the Cascades WIC Services Worksheets](#) to collect participant information.

- We recommend keeping copies of the Guidelines, WIC Certification Worksheets and pertinent forms like the Rights and Responsibilities available for these situations.
- D. Enter the information in Cascades within 2 business days.
- E. Scan the worksheet and any attached forms into Cascades and destroy the paper copies.
- Examples include: the Rights and Responsibilities form, Medical Documentation Form, Affidavits for Income, Id or Residency, etc.
- F. Offer the option to come to the clinic to receive the WIC Card when Cascades is available, or mail the card to the participant.
- See [Volume 1, Chapter 22 - Issue WIC Food Benefits](#) for more information.
- G. Issue benefits and notify the participant when available.

POLICY: Electronic Benefit Transfer (EBT) Provider is Unavailable

Staff must contact Cascades Support when it appears the EBT system is down. For example, when there are problems issuing a WIC Card, food benefits or participants report having difficulty purchasing foods at the store.

Cascades Support contact information:

- Call: 1-800-841-1410, press 3, then 2
- Email: Cascades.Support@doh.wa.gov

PROCEDURE:

Staff follow procedures according to the following:

A. Problems issuing a WIC Card:

- Contact Cascades Support.
- Offer to have participant pick up the WIC Card when the EBT provider is available again or mail the card to them.

B. Can't issue food benefits:

- Contact Cascades Support.
- Issue benefits remotely when able and staff sign their name (staff's name) along with the initials R.B.I. for remote benefit issuance.
- Contact the participant when food is available in the Electronic Benefit Account (EBA).

C. Participant reports issues purchasing foods at store:

- Have the participant use the [WICShopper app](#) "I couldn't buy this" button to notify us of the food item.
- Call WIC at 1-800-841-1410 and ask for Cascades Support.
- Email WIC foods at wawicfoods@doh.wa.gov.
 - o Please include the following information:
 - o Store name and location.
 - o Food item name.

- o Package or container size.
 - o UPC code (12-digit number listed under the food item barcode).
- Contact the participant when the issue is resolved, as appropriate.

Section 6: Appendix

EXAMPLE: Cellular Device Authorization and Agreement

1. Business Need

Supervisors must ensure cell phones and service plans are necessary for business needs.

The issuance of a cell phone is based on: (check all that apply)

- Employee's job requires field or remote work or travel.
- Employee's job requires immediate or on-call availability.
- Employee's job requires real-time communication, including email or chat.
- Employee needs a cellular device for safety, security, or other emergency reasons.
- Other:

2. Employee Agreement

- I agree to follow my agency's Cell Phone Policy.
- I will have my cell phone turned on during my scheduled work hours **and/or**:
- I will have my cell phone turned on during these additional hours: _____

I understand and will comply with agency and federal laws including, but not limited to:

- Records requests and records retention.
- All agency and agency security policies and procedures.
- Device surrender if subject to public records requests or litigation.

EMPLOYEE SIGNATURE

[Position]

Date

AGENCY AUTHORIZING SIGNATUREDate

Washington WIC doesn't discriminate.

In accordance with federal civil rights law and U.S. Department of Agriculture (USDA) civil rights regulations and policies, this institution is prohibited from discriminating on the basis of race, color, national origin, sex (including gender identity and sexual orientation), disability, age, or reprisal or retaliation for prior civil rights activity.

Program information may be made available in languages other than English. Persons with disabilities who require alternative means of communication to obtain program information (e.g., Braille, large print, audiotape, American Sign Language), should contact the responsible state or local agency that administers the program or USDA's TARGET Center at (202) 720-2600 (voice and TTY) or contact USDA through the Federal Relay Service at (800) 877-8339.

To file a program discrimination complaint, a Complainant should complete a Form AD-3027, USDA Program Discrimination Complaint Form which can be obtained online at: <https://www.usda.gov/sites/default/files/documents/USDA-OASCR%20P-Complaint-Form-0508-0002-508-11-28-17Fax2Mail.pdf>, from any USDA office, by calling (866) 632-9992, or by writing a letter addressed to USDA. The letter must contain the complainant's name, address, telephone number, and a written description of the alleged discriminatory action in sufficient detail to inform the Assistant Secretary for Civil Rights (ASCR) about the nature and date of an alleged civil rights violation. The completed AD-3027 form or letter must be submitted to USDA by:

1. **mail:**
U.S. Department of Agriculture
Office of the Assistant Secretary for Civil Rights
1400 Independence Avenue, SW
Washington, D.C. 20250-9410; or
2. **fax:**
(833) 256-1665 or (202) 690-7442; or
3. **email:**
program.intake@usda.gov

This institution is an equal opportunity provider.
Washington WIC doesn't discriminate.

To request this document in another format, call 1-800-841-1410. Deaf or hard of hearing customers, please call 711 (Washington Relay) or email WIC@doh.wa.gov.

Service Interruption Action Plan

Problem	Step 1	Step 2	Step 3	Step 4	Step 5
<p>1. Electronic device or network failure This includes computer, signature pad/card reader, printer, mouse, monitor, keyboard, laptop battery, cables, and or network failure.</p>	<p>Contact Cascades Support staff (1-800-841-1410, option 3, then option 2) OR Contact HTS Service Desk (1-888-457-2467)</p>	<p>Assess the timeline for resolution to determine how to deliver services to participants. See Step 3.</p>	<p>Use WIC Services Worksheets if appropriate. Ask participants if they want to receive a WIC Card by mail or return to the clinic for a card after the clinic is on-line.</p>	<p>When system is functioning, enter certification information in Cascades.</p>	<p>Issue benefits remotely and notify participant they're available. Mail WIC Card if requested.</p>
<p>2. Software or Database Problems; SAW outage, EBT Provider Unavailable Application freezes or doesn't work; can't access Cascades because SAW is down, error messages; can't issue WIC card, etc.</p>	<p>Contact Cascades Support For database problems, don't continue to use Cascades.</p>	<p>Assess the timeline for resolution to determine how to deliver services to participants. See Step 3.</p>	<p>Use WIC Services Worksheets if appropriate Ask participants if they want to receive a WIC Card by mail or return to the clinic for a card after the clinic is on-line.</p>	<p>When system is functioning, enter certification information in Cascades.</p>	<p>Issue benefits remotely and notify participant they're available. Mail WIC Card if requested.</p>
<p>4. Power Outages- Any type</p>	<p>Notify HTS Service Desk and Cascades Support</p>	<p>Shut down all computers. Follow the HTS Service Desk direction. Determine whether clinic can continue to operate according to</p>	<p>Use WIC Services Worksheets if appropriate Ask participants if they want to receive a WIC Card by mail or return to the clinic for a card after the clinic is on-line.</p>	<p>When system is functioning, enter certification information in Cascades.</p>	<p>Issue benefits remotely and notify participant they're available. Mail WIC Card if requested.</p>

		agency policy and safety issues.			
5. Natural Disasters Flooding, earthquake, storm damage, fire, or other acts of nature.	Follow agency's procedures in reporting natural disasters to appropriate authorities. Notify HTS Service Desk and Cascades Support	Determine whether clinic can continue to operate according to agency policy and safety issues.	Notify the LPC if the natural disaster has impacted or stopped delivery of WIC services	Use WIC Services Worksheets if appropriate Ask participants if they want to receive a WIC Card by mail or return to the clinic for a card after the clinic is on-line.	When system is functioning, enter certification information in Cascades. Issue benefits remotely or ask participant to return to clinic.