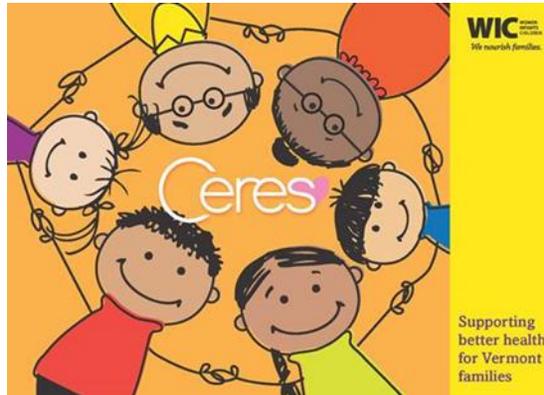

Vermont Department of Health



State of Vermont **Vermont WIC MIS/EBT Implementation**

Security Plan

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

Revision History

Version	Date	Author(s)	Revision Notes
1.0	11/4/11	Nancy Rowell	Draft Created
1.1	12/15/11	Nancy Rowell	Updates after K. Rowley State Security Review
1.2	1/21/13	Nancy Rowell	Update per D. Prail
1.3	7/22/13	Nancy Rowell	Update per MPSC system standards
1.4	12/30/13	Nancy Rowell	Addition of Ciber information, AHS edit
2.0	2/7/14	Nancy Rowell	Incorporation of DII & AHS determinations
3.0	6/11/14	Nancy Rowell	Addition of Xerox information
3.1	7/14/14	Nancy Rowell	DRC (QA Review) edits – hyperlink properties updated and 14.12 reference to “following contract signing” removed. 11.1 updated to reflect new NIST upgrade.

Table of Contents

1	VERMONT WIC MIS INCLUDING EBT DELIVERY SYSTEM	5
2	INFORMATION SYSTEM CATEGORIZATION	5
3	INFORMATION SYSTEM OWNER	5
4	AUTHORIZING OFFICIAL	5
5	ASSIGNMENT OF SECURITY RESPONSIBILITY	5
6	INFORMATION SYSTEM OPERATIONAL STATUS	5
7	SYSTEM TYPE	5
8	GENERAL SYSTEM DESCRIPTION/PURPOSE	6
9	SYSTEM ENVIRONMENT	6
10	SYSTEM INTERCONNECTIONS/INFORMATION SHARING	7
11	RELATED LAWS/REGULATIONS/POLICIES	7
11.1	NIST	7
11.2	SAFE AT HOME	7
11.3	WIC SECURITY REQUIREMENTS	8
11.4	ESTABLISHED POLICIES	8
12	DII CENTRAL HOSTING FACILITY	8
12.1	SOV SECURITY POLICY & PROCEDURES	8
13	CERES APPLICATION LEVEL	16
13.1	ENVIRONMENTAL SECURITY	16
13.2	INTERNET/ NETWORK SECURITY	18
13.3	DII HELPDESK OPERATIONS	18
13.4	SEPARATION OF DUTIES	18
13.5	DATA INTEGRITY	20
13.6	PATIENT PRIVACY	20
13.7	PERFORMING BACKUPS	20
14	WIC EBT (XEROX EPPIC)	21
14.1	WIC EBT APPLICATION REGULATION	21
14.2	RETAIL LEVEL SECURITY	21
14.3	XEROX ENVIRONMENTAL/PHYSICAL SITE SECURITY	21
14.4	XEROX HARDWARE SECURITY	23
14.5	COMPUTER SOFTWARE SECURITY	25
14.6	DATA ACCESS AND STORAGE	29
14.7	CLIENT/USER SECURITY	31

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

14.8 TELECOMMUNICATIONS SECURITY.....33

14.9 NETWORK SECURITY.....34

14.10 FISERV CARD PRODUCTION PROCESSING SECURITY.....35

14.11 ADDRESSING SECURITY DEFICIENCIES OR BREACHES37

14.12 ROLES AND RESPONSIBILITIES37

15 CERES TRANSFER & IMPLEMENTATION CONTRACTOR SECURITY 39

15.1 DATA CENTERS.....39

15.2 PHYSICAL ENVIRONMENT39

16 INFORMATION SYSTEM SECURITY PLAN COMPLETION DATE 43

17 INFORMATION SYSTEM SECURITY PLAN APPROVAL DATE 43

18 APPENDIX A GLOSSARY 44

19 APPENDIX B: REFERENCES 48

20 APPENDIX C: DII SOV POLICY 48

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

1 Vermont WIC MIS including EBT Delivery System

Vermont WIC Management Information system including Electronic Benefit Transfer Delivery System is comprised of:

- MIS System
- MIS-EBT Interface
- External EBT System/Host
- System Batch Messaging
- Windows Services

2 Information System Categorization

The FIPS 199 categorization ID for the MIS, i.e., catastrophic loss

- For the MIS and EBT is moderate if a Secretary of State “Safe at home” participant’s demographic data is compromised
- For the MIS and EBT is low for specific prescription data
- For the MIS is moderate for a participant’s personal health data.

3 Information System Owner

Vermont WIC Program, Maternal Child Health Unit, Vermont Department of Health, Agency of Human Services, 108 Cherry Street, Burlington, VT 05401, wicvt@state.vt.us, (802) 863-7508

4 Authorizing Official

Donna Bister, Donna Bister, Child Public Health Administrator, Vermont Department of Health, Agency of Human Services, 108 Cherry Street, Burlington, VT 05401, donna.bister@state.vt.us, 802-863-7508

5 Assignment of Security Responsibility

Jack Green, AHS Security Director, Division of Information Security, Department of Information and Innovation, 133 State Street, Montpelier, VT 05602, Phone: 802-585-6738, Fax: 802-828-1244, Email: Jack.Green@state.vt.us

6 Information System Operational Status

The operational status of the system is that it is in production in Colorado, Utah and Wyoming. The Vermont project began the Implementation phase in January of 2013, with Procurement of a QA, Transfer and Implementation and EBT service contractors. Procurement was completed 11/1/2013. The design/configuration phase was completed on 5/30/14. The Transfer Phase ends on 5/30/15, with pilot and rollout ending in full production in 3/2016.

7 System Type

- The WIC MIS system is a Management Information System application

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

- The WIC EBT system is a benefit delivery and vendor reimbursement system

8 General System Description/Purpose

Information Systems (IS) in the Special Supplemental Nutrition Program for Women, Infants and Children (WIC Program) support a number of program operations and management functions. The MIS/EBT system contains all business process, which certifies Vermont WIC participants, assigns benefits; transfers benefits and supports benefit redemption including the following:

- Appointment Management
- Caseload Management
- Certification
- Financial Management
- Food Benefit Issuance
- Food Benefit Redemption, Settlement & Reconciliation
- Nutrition Education, Health Surveillance & Referrals
- Operations Management
- Scheduling
- System Administration
- Vendor Management

The Functional Requirements Document for a Model WIC System (FRED) provides a comprehensive description of functions that are included in the WIC MIS.

http://www.fns.usda.gov/apd/WIC_FRED.htm

The approximately 160 Vermont state users and their user environments are varied. The user community ranges from Public Health Nurses at remote Clinic locations to the super users within VDH who must report to a federal level.

9 System Environment

The hardware system environment includes multiple locations for the WIC MIS and EBT. The central MIS hosting location at DII, the WIC Administrative site at the Vermont Department of Health and Clinic locations within State District Offices are all within state network control. Remote clinics in public facilities, the externally hosted EBT system and retail grocer locations throughout Vermont and including retail border grocer locations in New York, Massachusetts and New Hampshire function external to the state network.

The software includes at a minimum development, test, and production environments.

It would be helpful to have a training environment and a staging environment.

10 System Interconnections/Information Sharing

The systems below represent systems, which either require information from or send information to the WIC MIS system. None except the EBT systems are truly integrated and the data exchanges could be more accurately classified as data import/exports. Any Imports, Exports of data or new messaging functions are out of scope for the System Implementation project and will continue to be handled as they currently are to meet WIC business needs. The out of scope data exchanges are listed here as future system enhancements.

System Name	Organization	Type	Agreement Type	Date	FIPS 199 Category	C & A	Status
Medicaid	AHS				moderate		Out of Scope
CIS	AHS/DCF	Export			moderate		Out of Scope
IMR	AHS/VDH IMR	Import			moderate		Out of Scope
HHL PSS	AHS/VDH Lead	Import			moderate		Out of Scope
SNAP	AHS						Out of Scope
EBT Host	Xerox	Batch Messaging Windows services	Contract	1/2015	moderate		Development
Medical Providers	VITAL				moderate		Out of Scope

11 Related Laws/Regulations/Policies

11.1 NIST

The system was not specified to need NIST standards by the USDA FNS when it was developed for the USDA FNS. It does meet Federal security standards for WIC systems and the system will be hosted by the SOV under State Security rules. Per the AHS CIO NIST standards will not apply in this case at this time however the Ceres system is slated to be upgraded to fully comply with NIST 800-53 standards in October of 2014.

11.2 Safe At Home

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

The system must implement standards to protect and guard against the misuse of individually identifiable health information held or transmitted in any form or media, whether electronic or paper, at the record level.

11.3 WIC Security requirements

- Using Authentication controls (user ID and Password)
- Encrypting protected Health information (PHI) during transmission
- Having in place a comprehensive disaster plan
- Restrict access to PHI to staff who need it in order to perform job duties
- Intrusion detection capability for access to the network
- Administrator defined timing out of workstations to prevent unauthorized viewing of PHI

11.4 Established Policies

All established policies, procedures, and guidelines, whether they have been invoked by the USDA FNS, VDH IT, VDH, AHS, DII or State of Vermont policy

12 DII Central Hosting Facility

12.1 SOV Security Policy & Procedures

12.1.1 Introduction

There are two types of security to consider. Access to the State of Vermont’s information systems and computing resources will be based on each user’s access privileges and a user will be authenticated through Active Directory. Access privileges will be granted on the basis of specific job needs (i.e. a “need to know” basis). Access controls must ensure that even legitimate users cannot access stored information unless they are authorized to do so. All applications will have access controls unless specifically designated as a public access resource.

State of Vermont IT employees are responsible for maintaining secure access to the State of Vermont information systems and computing resources. Access permission levels will be determined by individual departments/agencies as employee supervisors deem appropriate.

The second is application-only. Security includes a user ID and password controlled by the application and based upon role based security.

12.1.2 Requirements

To support the Information Vermont State Security Policy, the following requirements are defined:

- Terminated employee, contractor, and vendor user accounts to all applications, systems, resources and physical access will be revoked, disabled and terminated immediately following exit.

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

- State of Vermont information must be protected from unauthorized disclosure, modification, or destruction. Information about security standards and practices must be implemented to ensure that the integrity, confidentiality, and availability of information are not compromised.
- All hardware and software used by the State of Vermont will be documented and in compliance with all State applicable standards and policies.
- Printed Documents that contain information that may be sensitive must be assigned a classification (confidential, private, and public) in order to determine the level of sensitivity in which they must be handled.
- Personnel who have access to sensitive information may require background checks or screenings. Screenings and background checks will be conducted per department/agency and DHR policy.
- Restricted areas within agencies/departments that house sensitive or critical information systems will at a minimum, utilize physical access controls designed to permit access by authorized users only.
- To maintain the availability, integrity and confidentiality of information, computer and communications equipment will be secured from physical and environmental threats.
- System capacity requirements will be monitored and usage projected to ensure the continual availability of adequate processing power, bandwidth, and storage.
- Agencies will establish internal procedures for the secure handling and storage of all electronically stored information that is owned or controlled by such agency.
- Users with access to State of Vermont customer sensitive information are strictly prohibited from downloading any customer information onto laptops, disk, flash drives, etc. unless the portable device is encrypted. Examples of sensitive information may be a combination of any of the following but not limited to this list:
 - Customer name
 - Mailing address
 - Email address
 - Phone number
 - Credit card information
 - Social Security Number
 - Health information
 - Banking Information

12.1.3 Data Centers

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

DII Data Center Locations

- 133 State Street, Montpelier
- McFarland House, Barre
- National Life, Montpelier

All locations are secure access facilities, not open to the public.

The main data center at 133 State Street is provided with an uninterruptable power supply and back-up generator to ensure up-time in the event of a prolonged power outage. The data center at National Life is the newest center. It provides an uninterruptable power supply and back-up generator. The data center at McFarland House in Barre provides limited space for disaster recovery of critical systems.

12.1.4 Physical Environment

Power supply

- Redundant UPS system
- Standby generator
- 24x7 power back up systems

Environmental Control

- Air-conditioned environment
- Temperature and humidity control and monitoring

Physical Security

- Electronic Key Access
- Multiple-zone access control
- Lockable cabinets and racks
- Unauthorized access alarm systems

Fire Suppression Systems

- Multiple zoned, pre-action dry pipe system

12.1.5 Types of Services

DII Technical Support Services offers a full range of information support through planning, evaluation, installation, tailoring, monitoring, diagnosis, maintenance, problem solving, training, security and administration of system control and third party programs. DII provides database and data storage management services. The following services are relevant to the MIS/EBT system:

- Physical spaces for computers, servers, peripherals, networking, telecom and other equipment

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

- Server Hosting
- Backups - A backup and recovery solution, Symantec Enterprise NetBackup will be built into the systems design and is included in the EA on Demand Infrastructure charges. WIC data is backed up and securely replicated offsite to DII's secured remote location utilizing Enterprise Data Domain with De-Duplication technology. The normal cycle is to keep backups for 14 days, making daily incremental and full weekly backups.
- Power and cooling for computers, servers, peripherals, networking, telecom and other equipment
- Physical security for computers, servers, peripherals, networking, telecom and other equipment, as well as data storage devices such as disk and tape volumes
- Server Monitoring and Alerting - Monitoring and troubleshooting and customer support services, 6 AM-12AM, M-F. Monitoring and back up call support off hours. Monitor system consoles for performance, system errors and job failures. DII's server monitoring service utilizes Microsoft's System Center Operations Manager (SCOM) to watch primary domain servers. In addition to SCOM, DII uses Solar Winds for system monitoring and threshold alerting for systems that are not within SCOM's domain boundary.
- Remote job operation services
- Job scheduling, library, and quality assurance services
- Server Antivirus and Multi-Tier Protection
- Server Maintenance, Patching and Updating
- Active Directory Services - Active Directory Services (ADS) is a manner to service all who login to a computer upon accessing the DII/SOV network. Authentication for the network is provided by AD. AD lets the computer know whether the requestor has the access to log on or not from any particular computer. ADS shares information to those who have the permissions to it. This includes printers throughout DII/SOV. After a successful authentication, ADS can shield sensitive data from unauthorized access.
- SQL Administration & Support
- Server Configuration Support (DNS, DHCP, WINS)
- Mobile Device Support

Software supported on DII enterprise servers:

- DFSMShsm (Hierarchical Storage Manager) is an optional feature providing backup, recovery, migration, and space management functions.
- RACF (Resource Access Control Facility) is IBM mainframe security software that verifies user ids and passwords and controls access to authorized files and resources.

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

- TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can be used as a communications protocol in a private network (either an intranet or extranet).
- Connet:Direct provides the capability for moving mission-critical data to and from a variety of platforms supporting multiple communication protocols.
- VTAM (Virtual Telecommunications Access Method) is an IBM application program interface (API) for communicating with telecommunication devices and their users.
- NETVIEW is IBM's network management system. A text message-based system that monitors, manages and controls SNA networks.
- TSO/ISPF is an IBM text editor and programming facility.
- QWS3270 is a standards compliant TN3270 emulator application.
- Zeke is an automated job scheduler and monitor.
- TMON offers detailed monitoring of operating system performance.
- CA TLMS Tape Management is an automated tape management system, which controls and protects z/OS tape volumes and data sets.
- VM/ESA is an IBM operating system capable of running multiple systems, with each running its own programs.

12.1.6 Data Center Access

The DII Data Centers provide a 24x7 high availability, redundant, and secure environment for all systems in compliance with HIPPA and other regulations as may exist.

The DII Data Centers are intended to enable systems administrators of the servers housed in a Data Center to be able to effectively manage their machines remotely and securely. All personnel must have proper authorization to obtain access to any of the DII Data Centers.

Authorized individuals will have unassisted access to the DII National Life Data Center 24 hours a day. Every authorized individual will have National Life access cards assigned to them that will allow them entrance to the National Life facility when needed. The National Life access cards are issued by National Life, but preliminary authorization is granted by the DII Data Center management. The process to acquire authorization for each level is detailed below. All persons requesting access to the DII Data Center must have proper authorization. A Data Center authorization form must be on file for each person who is requesting authorization to enter. This file will be maintained by DII staff. DII will notify BGS Security to remove authorization of employee access if there is a job change or termination of employment or if there is found to be a violation of any DII Data Center rule.

Visitor Guidelines

Anyone who does not have an authorization card is considered a visitor. This includes state personnel without an approved authorization and all vendor staff. Visitors must be accompanied

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

at all times by an authorized employee while in any DII Data Center. Visitors must log in and out when entering and exiting the DII Data Center. The purpose of the visit must be documented as part of the log in process. All visits to the DII Data Center are scheduled through the DII Data Center Management at least 24 hours in advance. Please contact DII-DataCenterManager@State.vt.us to arrange for a visit.

Authorization Process

An employee requiring access to any DII Data Center must receive authorization by Data Center management. Please contact DII-DataCenterManager@State.vt.us to request authorization. Once approved, the employee's name will then be added to the authorization list and the employee will be given an access card.

Audit Procedures

- The Data Center Manager will send a list of authorized employees to each manager on a regular basis for review and verification.
- The manager will review and update the list of authorized employees and return it to the DIIDC Manager within two weeks.

12.1.7 Data Center Rules

- No food or drink is allowed within the DIIDC.
- No hazardous materials are allowed within the DIIDC.
- All packing material must be removed from computer equipment and/or components in the specified staging areas before being moved into the DIIDC. This includes cardboard, paper wrap, peanuts, plastic, wood and other such material.
- No cleaning supply is allowed within the DIIDC without prior approval. This includes water.
- Only HEPA filter vacuums may be used inside the DIIDC.
- No cutting of any material (pipes, floor tiles etc...) shall be performed inside the DIIDC unless special arrangements are made.
- Employees shall only access racks that contain equipment for which they are personally responsible.
- All persons must stay in their designated area.
- No person is to interfere with any equipment not managed by them.
- No person is to interfere with data center operations.
- Only DIIDC staff shall access the sub-floor or remove floor tile.
- All persons must wear their ID and it must be visible at all times.
- All problems and/or concerns will be communicated to the DIIDC staff.

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

- In the event of an emergency, notify DIIDC staff immediately.
- All areas, including workstation, will be kept clean and organized.

12.1.8 Equipment

DII

In order to enhance security and reduce the chance of disruptions, the following policies apply to all equipment housed in the DIIDC.

- An equipment form must be completed for all equipment installations and removals.
- Equipment forms can be obtained online or by contacting the DIIDC Manager.
- DIIDC employees will deny access to anyone who intends to install or remove equipment without an installation form on file.

The DIIDC is intended to be a limited physical access location for servers. Systems administrators of machines, which are housed in the DIIDC, must plan their servers as if they will only get physical access to them when it is necessary to perform hardware modifications or replacements.

Servers will be configured with secure access administrative tools to allow for remote maintenance. All machines in the DIIDC must be rack mountable.

All new systems to the data center must undergo a security scan or audit prior to install. While the DIIDC provides increased network security, it is still necessary to take care of host-based security policies. Hosts in the DIIDC will be scanned regularly for vulnerabilities and those reports provided to the appropriate personnel. A security plan must be submitted to the DIIDC manager.

All new systems and hardware to the DIIDC will need to be coordinated and scheduled with the DIIDC staff.

NO equipment may be placed outside of the designated rack.

NO objects may be placed on top of or next to a rack on the floor.

Portable Equipment

Portable equipment such as notebook computers should be fitted with locks designed for notebooks, and secured to a desk whenever possible.

- Unattended notebooks and portable equipment will be stored in a locked cabinet or room.
- Notebook computers will not be left in vehicles unless locked in the trunk out of view.
- Notebook computers will be protected from excessive heat and cold.
- Notebooks will be returned to the home clinic after use at remote clinics.

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

- Notebooks or portable devices will not be serviced or sent to surplus unless authorized by AHS IT.
- Only State of Vermont authorized notebook computers with ability to encrypt data will be used for remote WIC Clinics.

12.1.9 National Life Additional Data Center Rules (DII NLDC)

Access

- National Life issued photo access card is required for access.

Equipment

- Do not carry any equipment larger than a laptop.
- For larger equipment, please contact National Life Security for separate entrance access. Please allow 24 hours advanced notice.

12.1.10 Hardware/Software Maintenance & Upgrades of Production Equipment

Authorized personnel may perform maintenance and/or repairs on equipment on an as-needed basis as approved by the DIIDC Manager.

12.1.11 SOV Network

The DII Network Engineering (NE) has the primary responsibility for the design, service and management of the State of Vermont’s Wide Area Network (WAN), Metropolitan Area Network (MAN) and Data Center network infrastructure. The group interacts with all State entities providing connectivity solutions for all site locations with an expected standard of 99.99% availability.

Network Engineering works in conjunction with State agencies and departments to design connectivity solutions to ensure business and system performance requirements are met. NE functions in a unique position as the mid-point to all State of Vermont network communication. This central vantage point allows NE to provision end-to-end service needs for large projects as well as be a valuable resource to departments needing network assistance or diagnosing LAN events. One such service is a “virtual” firewall service that is a unique offering for departments without the need to purchase additional hardware.

Network Engineering monitors and manages the daily operations and network health from a centralized operations center in Montpelier and works at levels II and III of the triage process within DII. Service and project requests are processed through a centralized work order system to efficiently route work requests to the appropriate team. The NE group provides network/system monitoring and alerting services for departments and provides a custom department monitoring web portal.

DII Network Engineering

- Maintains DNS services for a majority of the State of Vermont’s domains
- Maintains several layers of network firewall systems

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

- Maintains monitoring services that continually watch the stability of the State's Network Infrastructure

These systems are capable of monitoring not only network equipment but also systems like HVAC, UPS, power distribution units, Servers, phone systems, etc. With these systems, Network Engineering creates monitoring portals and alerting services for agencies and departments to present a single status tool for their network health.

Network Engineering employs Intrusion Detection Systems (IDS) and other systems that monitor potential hostile traffic on the network. These systems can be leveraged for compliancy and security enforcement.

Purposes for monitoring systems:

- Stability of systems and services running on the network both Local Area Networks (LAN) and Wide Area Networks (WAN)
- 24 / 7 / 365 alerting of events to create efficiencies of not staffing around the clock
- Mean Time to Recovery (MTTR) is significantly reduced when devices are monitored to show timing, and relationships of alerts.
- Compliancy to regulatory guidelines often requires monitoring at several layers to be in compliance.
- Automated response to monitored events is critical in maintaining stability through malicious attacks. Without monitoring and evasive action taken promptly, a domino effect can cripple network environments.

12.1.12 State Continuity of Operations Plan (COOP)

State of Vermont COOP plans are available at www.VermontCOOP.com via secure access.

13 Ceres Application Level

13.1 Environmental Security

All WIC Local Agency physical locations are within one of the 12 State of Vermont District offices and governed by the State of Vermont Agency of Human Services Policies and Procedures as well as State of Vermont Policies and Procedures.

- Locations are climate controlled
- Locations have lockable closets and cabinets for EBT Card stock and equipment security
- Equipment located in areas accessible to clients and/or the public will be properly secured to prevent tampering or accidental interruption of service.
- AHS network automatically locks the user screen after a set period of time, however processes run in the background when the screen is locked. This process does not affect after hours WIC synchronization processes.

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

- Vermont Department of Buildings and Grounds (BGS) maintain Security for the District Office Buildings, which have electronic key lock entry
- Users logoff or turn off their computers/workstations when they will be away for any period of time
- Computers/workstations, servers and telecomm closets are kept clean and free of dirt, dust, and food
- Components are protected by surge protectors or line conditioners

Disaster Emergency Action Policy

Disaster Emergency Action Policy is governed by BGS and located here -

<http://bgs.vermont.gov/sites/bgs/files/pdfs/security/BGS-SEC-Vermont-ASAP-Manual.pdf>

District Office Disaster Recovery

Disaster Recovery is captured in the State of Vermont COOP plan and certain specifics are particular to each location, however the following apply to all locations:

- Key Access Card Reader System – The ProWatch Database handles the card reader key system in multiple buildings throughout the State. Card readers store information (can be disconnected from the network) and the card readers will still work. The File Server is in a DMZ -- behind a firewall. The system is backed up nightly and tapes stored off site.
- Exchange Email System -- DII Exchange email system for multiple departments and agencies. This email system is backed up and maintained by the Department of Information & Innovation.
- Telecommunications – The Centrex phone system for State Government & all district offices. This system is maintained by the Department of Information & Innovation.
- Wide Area Network (WAN) - The data circuits that connect Vermont's Wide Area Network provides network connectivity and Internet access for all district offices. The Department of Information & Innovation is responsible for maintaining and backing up this network.
- IT databases - All IT databases are on secure servers at DII or VDH.

Each location's COOP maintains the following:

Annex A - Teams and Responsibilities

Annex B - Alternate Facilities

Annex C - Mission Essential Functions

Annex D - Orders of Succession

Annex E - Delegations of Authority

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

Annex F - Alert Notification Procedures

Annex G - Vital Records / Resources

Annex H - Drive-Away Kits

Annex I - Communications

Annex J - Security Access Control

Annex K - Family Disaster Plan

Annex L - Devolution

Annex M - Test, Training, and Exercise

Annex N - Facility Evacuation

Annex O - Contacts Roster

Annex P - Pandemic Planning

Annex Q - Risk Assessment

Annex R - Risk Specific Action List

13.2 Internet/ Network Security

All District Office Clinics have web access via the AHS network. The network has a robust set of monitoring tools including On-access McAfee Scanning using the Enterprise Edition. Laptops used for remote locations will have state virus control installed. The antivirus software is configured so that virus definition automatically update without user interaction. AHS IT has the responsibility to assure firewall protection.

13.3 DII Helpdesk Operations

DII has a Helpdesk available by e-mail or phone, with ticket functionality for IT problems. The response time to tickets is tracked for constant improvement. Specific ticket problems are routed to the subject matter expert (SME).

13.4 Separation of Duties

Role Based

- All users will log into the Vermont State Network with State supplied credentials.
- The system must employ a role-based security that allows user access to application functional areas based on user security level. Roles will include but not be limited to public (For applications, etc.), Clinician, DO admin. State Admin.
- The system will allow users to have more than one role.
- The system administrator will be able to add and edit permissions for system access.
- The system will have the ability to support file, record and field level security.
- Security will be available to all modules and integrate with network operating security

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

13.4.1 Create Role Profiles

- The system must employ a role-based security that allows user access to functional areas based on user security level. Roles will include but not be limited to public (For applications, etc.), Clinician, DO admin. State Admin.
- The system will allow users to have more than one role.
- The system administrator will be able to add and edit roles for system access.

13.4.2 Create User Profiles

- The system will have the ability to support various levels of access by authorized users.
- The system will allow users to have more than one role.
- The system administrator will be able to add and edit permissions for system access.

Note: The WIC System application security is role based within the application as specified in 13.4.1. The WIC System does not support User Profiles or any profiles outside of the application.

13.4.3 Passwords

Password standards are set at the State level by DII.

Password Development

- Service account passwords will be changed a minimum of every sixty (60) days
- Service account passwords shall be a minimum length of eight (8) characters in a combination of upper and lower case alpha, numeric, and special characters.
- Default vendor passwords shall be changed during or immediately after installation of the information system product.
- Password changes shall be systematically enforced where possible.
- Accounts shall be systematically disabled after ninety (90) days of inactivity to reduce the risk of compromise.

System Password Protection

- Passwords are to be treated as confidential information. Under no circumstances is an employee to give, tell, or hint at a system password to any unauthorized person(s). Since systems are managed by more than one person, passwords shall be administered on a need-to-know basis only. If system passwords are “predetermined or sequential” they are to be kept locked in a secure area at all times.
- Passwords shall not be transmitted electronically over the unprotected Internet, such as via e-mail.
- No employee is to keep an unsecured written record of passwords, either on paper or in an electronic file unless kept in a controlled access safe or an encrypted file.

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

- If an employee either knows or suspects that a system password has been compromised, it must be changed immediately and reported to the IT department manager.
- If an employee terminates employment, it is necessary to change system passwords that the employee has knowledge of. Each agency/department is responsible for documenting these requirements within their written procedure.

All users of the MIS system are state employees and currently trained in the above procedures and rules.

13.5 Data Integrity

13.5.1 Data Conversion

Data conversion and migration is the responsibility of Ciber, the Transfer and Implementation (T&I) contractor. DII who hosts and maintains the current WIC application will oversee data conversion activities. Some conversion activities will occur within DII physical security and under DII security Policy and Procedures. Some conversion activities will occur at the Ciber facility. For information on Ciber's physical security and Security Policy and Procedures, please see Section 15.

13.5.2 Data Entry

Data integrity at the WIC clinics will be maintained at both the record and field levels within the centralized database. Data input will occur mainly at the Clinic level and proper training is imperative to maximize data integrity.

All staff scheduled to use the system will receive intensive training. Training will lessen the risk for erroneous data entry or accidental misuse that might compromise data integrity. For more information, refer to the Training Plan.

13.6 Patient Privacy

Computer monitors in clinics will be located to allow viewing by authorized personnel and participants but positioned to eliminate viewing by unauthorized persons.

13.7 Performing Backups

The system will save a backup of production data hourly and make the data available for immediate restoration for 30 days after the date/time of each back-up. The backups will be stored on media for offsite storage after 30 days.

Backup and recovery services are provided by NetBackup, which can be managed by designated NetBackup System Administrators. The NetBackup application and database components are installed on separate servers (Master & Multiple Media Servers), plus a HP MSL4048 2 Ultrium960 Tape Drive, in the SOV Enterprise NetBackup Environment, as part of an HP EVA 8000.

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

SOV Enterprise Backup/Recovery Services provides a complete and flexible data protection solution for a variety of platforms, including Microsoft Windows, UNIX, Linux, and NetWare systems. Also included is the support for leading database engines like Microsoft SQL Server, Sybase and Oracle; providing near real time database protection.

14 WIC EBT (Xerox EPPIC)

14.1 WIC EBT Application Regulation

WIC EBT application security is regulated by the USDA FNS WIC operation rules, Electronic Funds Transfer (EFT) standards, NACHA's Quest Operating Rules, FNS EBT rules and regulations, and Federal code 7 CFR 274.8(b)(3), which provide policies and guidelines for fraud prevention and overall administrative, physical, technical, and system security.

All Xerox Team facilities have operational security and risk management or reduction plans and procedures in place. The WIC EBT system (EPPIC) infrastructure is designed to incorporate rigorous security measures that restrict access to sensitive but unclassified information, such as cardholders' personal data and benefits information, only to authorized cardholders and State, federal, and Xerox employees.

Xerox adherences to Section 552a of Title 5, United States Code (the Privacy Act). EPPIC is unique in the industry as it was specifically designed for electronic benefits distribution and redemption. EPPIC's operating environment conforms to all EBT, WIC EBT, and credit card industry standards, USDA FNS requirements and guidelines, and Quest Operating Rules.

The Xerox Team has completed all state and federal audits in EBT/WIC EBT and state/federal treasury program operations. Procedures comply with federal requirements and guidelines and SSAE 16/SAS 70 audit specifications

14.2 Retail Level Security

14.2.1 Point of Sale (POS) Terminal security

Participants access to their benefits through POS terminals located at WIC authorized retailers. Benefit transactions performed through online processing will use a central processor to verify PINs and authorize transactions. Retailer requirements include cashier ID and password verification, settlement controls and integrity of transmitted data.

14.3 Xerox Environmental/Physical Site Security

This section describes environmental and physical site security measures taken at the Xerox data center.

14.3.1 Power Systems

The data center is equipped with reliable and fault-tolerant electrical sources to ensure continuous power to the facility.

A 625 KVA 60-cycle battery-operated UPS system services the computer rooms. The current consumption of the 625 KVA units is approximately 10 percent to 15 percent. This unit is

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

operational from a single module. The battery backup for the 625 KVA UPS provides enough power to operate the EPPIC computer systems for five minutes at full load.

The UPS system is serviced by three redundant battery banks. The batteries provide the voltage necessary for the UPS system to deliver continuous power for electrical requirements until the diesel generator and switch gear are fully engaged to provide alternate power, or until the city-supplied electrical current is restored.

To prevent overheating, the self-contained UPS room is serviced by two independent refrigerant systems that are rated at 15 tons each.

A 1500 KW diesel-powered electrical generator is maintained at the data center. The capacity of the fuel tank is 10,800 gallons. When city power has been out or significantly reduced for more than five seconds, the UPS automatically sends a signal to the generator to power up. No human intervention is required.

14.3.2 Physical Site Security and Policies Procedures

Physical site security at the data center is maintained not just through equipment but also through the enforcement of security policies and procedures.

Facility Walk-throughs - The facility walk-through is conducted by facilities personnel at least twice daily. This process includes inspection of many of the physical security areas described above, including the dock doors, computer rooms, UPS room, and cage area. Times at which walk-throughs are conducted are randomized to make it more difficult to plan unauthorized entry attempts.

Food/Liquid/Combustibles Ban - Personnel are strictly forbidden to bring food, drinks, or combustible materials into the computer rooms or electrical areas. This reduces the chance of problems being caused by contaminants in electrical contacts.

Key/Combination Control - Keys to padlocks and doors are stored in a safe. The safe combination is kept secure by the Xerox data center manager.

Visitor Control - Visitors must be authorized to enter the facility. All visitors must sign in with the receptionist in the foyer, be assigned a visitor badge, and be admitted by the receptionist with the remote door release. Visitors must be escorted at all times. The escort is responsible for ensuring the visitor returns the visitor badge at the end of the trip.

Before opening the door, the receptionist must announce to all center personnel that a visitor is in the building, so they know to take measures to ensure no sensitive data is visible. Before a visitor can be admitted to the computer room, personnel in that room must be alerted so they can cover or otherwise hide any sensitive data.

Equipment Inventory Tracking - All equipment in the data center is recorded in a program-specific inventory database. This log is reviewed and equipment is inspected biannually to identify theft or damage.

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

Equipment and Materials Storage - Unused equipment and materials that require secure storage are kept in the locked cage area.

Items that must be kept in the cage area when not in use include, but may not be limited to:

- Spare or replacement computer and network equipment (hard drives, routers, etc.)
- Installation sets of software used on workstations in the data center
- Removable recording media (diskettes, CDs, DVDs, backup tapes)
- Tools/equipment that can be used to open or work on computers
- Documents that contain sensitive information

14.3.3 Data Center Electronic Security

Daily maintenance of electronic security is the responsibility of the following Xerox staff: Lead Systems Administrator, Lead Network Administrator, and Operations Manager.

As an additional security measure, system modifications, whether hardware, network, or software modifications, require prior security approval and change management approval.

Procedures are designed to limit system access to authorized users only. Duties are segregated as much as possible to reduce the level and scope of access required by employees to do their jobs. Access privileges of employees who are terminated are removed at that time. Access privileges of employees who leave voluntarily are removed as a check-mark step in the employee exit process – i.e., before the employee has left.

14.4 Xerox Hardware Security

14.4.1 Use of Identification Badges

All employees of Xerox and subcontractors are required to carry electronic cards, which provide limited access to the facility in accordance with the employee’s job responsibilities.

14.4.2 Data Center Access Control

One of the primary means of securing the data center is by limiting access to the facility and to the sensitive areas within it.

The front door is the only entrance to the data center for personnel and visitors alike. That door allows entrance to a foyer, not to the interior of the building. From there, personnel must have a key card to be able to open the interior door. Visitors must be assisted by the receptionist.

Except on weekends and holidays, the front door into the foyer is unlocked from 7:30 a.m. to 5:00 p.m. daily. Personnel and visitors can freely enter the foyer during those hours.

The front door is automatically locked between the hours of 5:00 p.m. and 7:30 a.m. and at all hours on weekends and holidays. During those hours, personnel must have a key card to enter the building. All others can contact personnel inside the building through an intercom unit.

Key Card System - Doors to the data center are secured by an electronic card reader system. Secure areas inside the building are divided into access zones, and all doors to these secure

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

areas are controlled by key cards. Access cards are authorized, ordered, and distributed solely by the data center program manager. Key cards provide four levels of access, so personnel can be granted access consistent with their needs. Access activity for each key card is monitored automatically and reported monthly in a security log, which is reviewed by the facilities coordinator and the data center program manager. These logs provide time-stamped details on all zones accessed with each key card. The data center program manager will review the key card access logs at least once per month.

Intrusion Alarms - The data center is armed with monitored intrusion alarms that are monitored by a security company. Forced entry into the facility sets off an alarm, and the security company alerts the police.

Exit Alarms - The data center emergency exit doors have alarm systems. Opening these doors sets off a local alarm indicating an unauthorized or emergency exit.

Dock area - The dock area has two metal roll-up doors where pickups and deliveries are made. These doors can be opened only from the inside opened only by direction of the data center program manager, and must be left open for the minimum time possible.

Computer Room - To access the computer rooms, personnel must either have a key card authorized for computer room level access, or they must be escorted. The computer room is staffed and monitored by personnel 24 hours a day, 365 days a year.

Before a visitor can be admitted to the computer room, personnel in that room must be alerted. When a visitor is present, computer room personnel must turn off computer monitors, cover documents or put them in closed drawers, or otherwise hide any sensitive data.

Printers - Printers are located in secure areas such as the computer room, to limit access to potentially confidential documents that may be printed. Operations personnel check print-outs routinely to make sure the printers are functioning properly.

Cooling Towers - The cooling towers are enclosed in a locked fence. Access to the cooling towers is limited to personnel who are authorized by the data center program manager as having legitimate business needs in the area.

UPS Room - The UPS room is locked at all times. Access is key controlled and is limited to personnel who are authorized by the data center program manager as having legitimate business needs in the area.

Backup Generator - Access to the generator and its fuel tank is controlled by padlock and limited to the vendor that maintains the generator, and other personnel who are authorized by the data center program manager as having legitimate business needs in the area.

Cage Area - Inside the building near the dock doors is a locked cage area used for secure storage. Access to this area is key-controlled. Inside the cage area is a fire-proof combination safe and a number of locking cabinets for additional secure storage.

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

14.5 Computer Software Security

EPPIC transmits and stores highly sensitive financial and individual identity data. Because it interfaces with numerous stakeholders and transaction devices including system and database administrators, system and support personnel, State staff, cardholders, retailers, and third party processors, a strong security mechanism to maintain the system and data integrity, guarding the sensitive information is needed.

EPPIC supports authentication, integrity and non-repudiation. It includes numerous features to ensure the system is accessed only by authorized personnel, safeguard data transmissions, and provide means to monitor activities in the system.

14.5.1 Auditing and Monitoring

Audit trails provide additional system security for the EBT system. EPPIC tracks all root-level activities on the servers and keeps detailed records. EPPIC runs file-monitoring software that keeps track of all changes to all critical files such as password files, configuration files, and the audit trail files. Xerox compliance with annual SSAE-16 audits provides ongoing certification and examination of Xerox operations and control system.

14.5.2 Logging

Non-repudiation is provided in EPPIC through extensive auditing logging. Every action done by an authenticated user is logged in the database. As the logging is part of a distributed transaction, the audit trail is duplicated on multiple databases and disks. The data is easy to retrieve and analyze because it is stored in a relational database.

14.5.3 Administrative Terminal Security

EPPIC provides a robust, multi-level security system to tightly control access to administrative functionality. Administrative terminal security screens provide security administrators and designees a powerful, easy-to-use security management tool. Xerox highly configurable user profile approach gives the State significant flexibility in defining roles and access rules today, and this will continue in the new contract.

The State-defined user profiles are based upon a specific set of administrative terminal functions required by users to perform their respective jobs. As each administrative terminal user is granted access, the user is assigned a specific user profile based upon the job requirements. Those profiles determine which types of information users can view and which administrative functions users can perform. The State can create new profiles or modify existing profiles at any time as needs change.

EPPIC uses a multi-level security structure consisting of user types and roles, and user logins, to assign a security level to each individual user. The final set of functions accessible by each user is the aggregate of type and role functions. Using role-based access control allows the State maximum flexibility and control over system access.

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

14.5.4 User Management

To provide authentication EPPIC uses role based access controls.

EPPIC has security screens that allow the security administrator/designee the ability to assign security access to all users. These screens are accessible only for users who have the correct security clearances. The security administrator/designee uses a combination of user types and roles to define the access conditions for each individual worker or stakeholder.

There are no physical limits to the number of user types or roles, but it is most efficient to limit the numbers of categories. The user is assigned a user ID and password which grants access to the specific functionality assigned by the security administrator/designee.

14.5.5 Password Management

Upon accessing the system for the first time, the user is required to change the initial password before being allowed to proceed to the main screen, to ensure the initial password is not compromised. EPPIC forces the user to change passwords every so many days, as determined by the state.

EPPIC enforces a password lockout rule – when a user enters three invalid password entries, the system locks out that user to prevent further logins.

Administrative terminal user passwords are stored in the database in one-way hashed form, which is not reversible. Because of this, the password is only known to the holder. Even the system administrator does not know the passwords of other users.

EPPIC enforces login and syntax rules, which make passwords harder to guess. User login IDs in EPPIC must conform to these rules:

- Login IDs have a minimum of four alphanumeric characters (letters and digits) and a maximum of 10 characters.
- Special characters such as the “at” symbol or underscore mark (@ or _) can be used – Vermont administrative terminal users can use email addresses as login IDs.
- Login IDs are not case sensitive.
- Passwords in EPPIC must conform to these rules:
 - Minimum password length is eight characters
 - Minimum of one lower case alpha
 - Minimum of one numeric
 - Do not require but allow upper case alpha
 - Do not require but allow special characters
 - Require password change every X days, as determined by the state
 - Allow repeat of password one year after initial use

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

Session Management - EPPIC remembers individual working sessions and forces users to re-authenticate to get the session back if a session is not active for a configurable period of time. That inactivity time is set for 15 minutes for Vermont users. It is used to enforce the navigation path restriction for different users. The session information is stored not only in memory but also in a distributed database, so session information remains intact even if there is a system fail-over or fail-back.

14.5.6 Transmission Security – Secure Sockets Layer (SSL)

EPPIC supports digital certificates and Secure Sockets Layer for all Web sessions for data integrity. By supporting all major Web browsers, EPPIC ensures that it can always run on the most robust and secure Web browser.

All file transmissions, such as card generation files transmitted to Fiserv, the Xerox card production subcontractor for card production, are fully encrypted using secure protocol.

14.5.7 Firewalls

Two hardware firewalls are used to form a Demilitarized Zone (DMZ). A DMZ protects valuables from direct exposure to an untrusted Internet environment. It is a network added between a protected network and an external network (the Internet) in order to provide an additional layer of security. A DMZ is one aspect of the Xerox application of defense in depth because it adds an extra layer of security beyond that of a single perimeter.

A DMZ separates Internet messages from directly referencing an intranet by isolating the machine that is being directly accessed from all other machines. The DMZ is the Web server, which acts as a proxy server to get recipient and retailer transaction history and balance information.

The firewall in front of the DMZ allows passage of only the minimum required traffic. For the EPPIC portal this is only TCP port 80 for HTTP and/or TCP port 443 for SSL (HTTPS). The firewall between the portal Web server and intranet only allows passage of messages from the EPPIC-defined private port and protocol.

14.5.8 Intrusion Detection System

Proactive monitoring of the system is as important as preventing un-authorized access. An Intrusion Detection System (IDS) is used to detect inappropriate, incorrect, or anomalous activity. EPPIC uses both host-based ID systems that operate on a host to detect malicious activity, and network-based ID systems that operate on network data flows.

There are multiple network-based IDS to monitor different sections of the network. There is a host-based IDS running on the EPPIC Host and Portal Server.

14.5.9 Digital Certificate and SSL

Digital certificates encrypt data using SSL technology, the industry-standard method for protecting Web communications. The SSL security protocol provides data encryption, server authentication, message integrity, and optional recipient authentication for a TCP/IP

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

connection. EPPIC uses 128-bit strong encryption, which refers to the length of the “session key” generated by every encrypted transaction.

In addition to login ID and password, EPPIC can be deployed requiring the retailer to present with EPPIC signed digital certificates for retailer authentication.

14.5.10 Security Reports

Security reports assist the State in managing access to the administrative terminal. These reports provide information on failed attempts to log on the administrative terminal, and user access definitions.

Access Definition Report

This report details each authorized administrative terminal user with the ability to access the EBT program data on the administrative terminal. The report details the level of access afforded the user through the administrative terminal.

Failed Logon Report

Xerox provides a daily report listing all users who entered an invalid password for their user ID while attempting to log on to EPPIC.

Administrative Activity Report

Xerox provides a monthly report listing administrative terminal activity by user. The report is generated a list of user ID and the activity taken by the user on the administrative terminal.

14.5.11 PIN Security

EPPIC ensures the confidentiality and security of the PIN during generation, issuance, storage and verification. PIN security meets all current DES encryption standards.

PIN Generation and Issuance. Cardholders can select their own PINs through the ARU.

The PIN is stored in the EPPIC database in encrypted form. No individual, including the EPPIC security administrator/designee, is able to view the PIN in clear text form.

PIN Verification. Before a PIN is verified, EPPIC verifies if the processor and terminal are valid. Then the PIN is decrypted using the shared session, or working, key with the processor or terminal. The PIN is encrypted again with a different key, and then the PIN is verified against the encrypted form of the PIN in the database.

PIN Fails. Cardholders are allowed a limited number of invalid PIN attempts in a day before the card is locked. This PIN fail count is set at four incorrect PIN entries.

A correct PIN resets the PIN fail count if the correct PIN occurs prior to the card being locked. Once the cardholder reaches the PIN fail threshold, any transactions performed using the card are denied due to excessive PIN fails, even if the cardholder uses the correct PIN from then on.

The first transaction after midnight resets the PIN fails counter (to 1 if it is an invalid PIN transaction, or to 0 if it is a valid PIN transaction).

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

EPPIC supports the ANSI standard triple DES encryption for PIN encryption. For Web-based traffic, EPPIC supports strong encryption at a key length of 128 bits.

The security service manages encryption, which is easy to update should a new ANSI encryption standard, such as Advanced Encryption Standard (AES), be adopted in the future. A pseudo-random process generates each key and key component.

In addition, per Xerox business-wide requirements, all computer hard disks are PGP encrypted.

Database PIN Encryption key. Encryption of the PIN in the EPPIC database uses a key called the PIN encryption key (PEK). This key is different from the encryption key used when the PIN is sent to EPPIC from a POS or other device. This means that unauthorized access of one encryption key does not endanger the other form of PIN encryption.

POS Encryption Keys - EPPIC and a processor, or POS, share a master key encryption key (KEK). The KEK is used for exchanging the session, or working, key that is used for PIN encryption and decryption when the PIN is sent to EPPIC from a POS or other device.

14.5.12 Laptop Encryption

In addition to the EPPIC security, Xerox requires portable hardware containing personal information to be encrypted. Company security policy requires all laptop hard drives to be PGP encrypted

Personal Information means information in any form (written, oral, or electronic) that could be used alone or with other information to identify an individual. Some information, such as a Social Security Number, can be used alone to identify an individual, and is therefore considered Personal Information. Other types of information, such as a zip code, must be combined with other data to identify an individual in order to be considered Personal Information.

There are a variety of types of data that, alone or in combination with other information, can be used to create Personal Information. These include, but are not limited to:

- An individual's name, address, ZIP code, email address, telephone and fax numbers
- All dates related to an individual (e.g., birth date, admission date)
- Account or card numbers identifying a specific individual's account, including financial accounts
- Tax ID or Social Security Numbers
- User IDs, passwords, and logins

This type of encryption dramatically reduces the chances of an individual being able to obtain any information from a laptop in the event that a laptop is lost or stolen.

14.6 Data Access and Storage

14.6.1 System Access Controls

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

Every user must have a valid user ID and a valid password in order to log in to a system. The systems administrator employs a variety of password security options, such as requiring a minimum length and setting expiration periods. In addition, a user access lockout rule is enforced. If users enter too many incorrect passwords, they are locked out as possible intruders.

14.6.2 Data Backups

The data center runs regular backups on all servers. There are daily backups kept locally in secure storage, and periodic backups that are kept offsite at a bonded storage facility.

A daily database dump is done on all EBT systems at the data center. This material is systematically stored, retained, and accessed only by authorized personnel when necessary. In addition, the fail-over machines at the Xerox alternate site in Pittsburgh, Pennsylvania, are kept current, immediately recording every transaction posted to the system at the data center.

14.6.3 Use of Identification Badges

All employees of Xerox and subcontractors are required to carry electronic cards, which provide limited access to the facility in accordance with the employee's job responsibilities.

14.6.4 Segregation of Duties

Each business unit or location implements only properly tested, unaltered, and approved modifications into production. Application development units will create isolated environments to maintain separation of duties between development, test [quality assurance (QA)], and production activities. At a minimum, the development and test (QA) environments will be isolated.

Application development units implement a process so that:

- Workers with access to application source code do not have privileges to move the results of their work to test or production environments.
- Administrators responsible for moving application source code or programs from one environment to the next have no access privileges to the file contents being moved.
- Separate access controls exist between the requestor (usually the programmer), the approver (usually a manager), and mover (usually a system or database administrator) for all moves into production.
- Application source code or programs move only forward from development to test, and test to production.

All access to the EBT environment is on a business need to know basis. Only people whose direct responsibilities require access are granted access. Xerox management maintains a matrix of all roles and privileges to allow for quick review of access to determine appropriateness of access. Access is subject to established policies and procedures and is audited on a regular basis.

14.6.5 Xerox Access Control Policies

Only authorized personnel are allowed system access, as previously discussed.

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

Computer Room Access Policies - Access to any customer or Xerox data facility is strictly regulated. Access is granted on an as needed basis.

Network Access User Management - To provide authentication with maximum flexibility and fine grain access control, EPPIC uses role based access controls along with type-based privilege inheritance. EPPIC has a separate security screen that allows the administrative security administrator/designee the ability to assign security access to all users. The security administrator/designee uses a combination of types and roles to define the access conditions for each individual worker or stakeholder.

Type - This is a high-level category that defines generic functions within the EBT system. Categories such as retailer, operations, State, local office and FNS staff may be considered appropriate types by Vermont.

Role - As stated, a role is job function a user may perform using EPPIC. Potential roles include administrative, clerk, supervisor, or other relevant functions. Users inherit privileges from the roles that they perform and the type each belongs to. Furthermore, besides the inherited privileges, other privileges can be added or removed for each user.

The ability to just view or modify and delete information on a particular screen is assigned through the user security level. Therefore, all users in a particular type may have access to the same screen and its information but certain individuals may have the ability to modify or delete the information whereas the other may only be able to inquire on the data.

There are no limits to the number of types or user roles but it is most efficient to limit the numbers of categories. The user is assigned a user ID and password that grants the user access to the specific functionality assigned by the security manager.

Mobile Computing Policies - Xerox workers traveling for any purpose are responsible for the security of information and equipment in their custody. Persons who are issued portable computers and who intend to travel for business purposes must be aware of the security issues relating to portable computing devices and implement appropriate safeguards to minimize risks.

14.7 Client/User Security

14.7.1 System Access Controls

As stated, every user must have a valid user ID and a valid password in order to log in to a system. The systems administrator employs a variety of password security options, such as requiring a minimum length and setting expiration periods. In addition, a user access lockout rule is enforced. If users enter too many incorrect passwords, they are locked out as possible intruders.

14.7.2 Auditing and Monitoring

Audit trails provide additional system security for the Vermont EBT system. EPPIC tracks all root-level activities on the servers and keeps detailed records. EPPIC runs file-monitoring software

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

that tracks changes to critical files such as password files, configuration files, and the audit trail files.

14.7.3 Xerox Personnel

Xerox and each of the subcontractors with access to EBT data maintain Human Resources departments responsible for benefits management, hiring policies and procedures, and general human resources administration. For Xerox, the Human Resources Department is in Dallas, Texas.

Xerox and all subcontractors adhere to the following procedures:

Employee Screening - An offer for employment is contingent upon the candidate meeting the following conditions:

- Proof of United States citizenship or unrestricted access to work in the United States
- Satisfactory completion of a background investigation, which may include, but is not limited to, verification of past employment and education
- An executed original of employee confidential information and non-competition agreement
- Personal Interviews - All applicants are interviewed in person at least once prior to being made an offer of employment.
- Personal and Business Reference Checks - All employees must submit to a background investigation, which may include but is not limited to, verification of past employment and education.

Employee Code of Conduct - All employees must agree in writing to abide by the company's Code of Ethics.

Reporting Security Violations - Any employee who may be aware of a potential security violation is required to report the potential violation immediately to management.

Personal Data Changes - All employees are required to report personal data changes to the human resources department within 30 days of the change.

Alcohol and Drug Abuse - All employees are prohibited from possessing, using, distributing, manufacturing, purchasing, dispensing, or selling illegal drugs. Engagement in any of these activities is grounds for termination. Employees undergo pre-employment drug screening before begin hired. Alcohol and drug abuse are covered by policies pertaining to the safety of the workplace.

Weapons - Weapons (includes, but is not limited to handguns, rifles, knives, brass knuckles, mace, etc.) are strictly prohibited at any time on Xerox property or on an employee's person while on duty unless specifically authorized and approved in writing by the Xerox CEO or worn by law enforcement personnel. Where local State law does not state otherwise, weapons are

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

not permitted in company vehicles or personal vehicles if the personal vehicle is on Xerox property or being used on company business.

Conflict of Interest/Ethical Conduct Agreements - All employees are subject to all internal policies pertaining to conflicts of interest and ethical conduct.

Confidentiality - All employees must sign a confidentiality statement verifying their awareness of the confidential or proprietary nature of its customer's information. Employees are required to hold all such information in confidence and do so even when their employment with Xerox or a subcontractor ends. This requirement is reviewed with employees during the exit interview.

Training and Performance Appraisals - Employee training is provided in accordance with job requirements. Performance appraisals are conducted annually for all employees.

Disciplinary Actions - Disciplinary action is taken swiftly as performance issues arise. Depending on the severity of the reported infraction, the manager may discipline the employee or the manager may work with the human resources department in reprimanding or terminating an employee.

Separation/Termination - All employers reserve the right to terminate an employment arrangement at any time, except as otherwise provided by law or the key personnel provision of the Vermont EBT contract. Access privileges of employees who leave voluntarily are removed in the employee exit interview process – i.e., before the employee has left. Access privileges of employees who are to be terminated are removed at the point of termination.

14.8 Telecommunications Security

EPPIC must interface with several different external entities necessary for transmitting files, transactions, and reports. The external entities that the Xerox host system interacts with include:

- Vermont Ceres system for batch files
- State staff using administrative terminals
- EBT-only retailers
- TPPs
- Interoperability gateway
- WIC vendors
- Cardholders
- Concentrator bank
- FNS for transmitting REDE, AMA/ASAP, STARS, and ALERT files

Xerox establishes all requisite communications to the State to interface with its eligibility system. Xerox establishes communications to diverse external stakeholders, including EBT-only

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

retailers, WIC vendors, TPPs, FNS, cardholders through the Internet, and Xerox client and retailer help desks.

14.8.1 Transaction Processing and Call Center Networks

For Xerox transaction processing and help desk networks, Xerox provides a telecommunications infrastructure to route around any failed circuit. Xerox uses MPLS for most of the data connection circuits, providing built-in redundancy, security, and reliability. MPLS offers performance and cost advantages and uses multiple protocols such as Ethernet, frame relay, ATM, and PPP. This provides inherent redundancies for re-routing transaction activity should a path become inoperable. Xerox provides primary and backup T1 lines for all communication links between the State offices and Xerox, as well as between the Xerox primary host processing facility in Dallas, Texas, and the Xerox hot backup site in Pittsburgh, Pennsylvania. Additionally, the ARU and call center is supported with a primary and backup T1 line.

14.9 Network Security

To operate the Vermont EBT host system, Xerox establishes an electronically secure interface for receiving and transmitting local and batch data from the State’s central and local offices where required. The secure, automated data connection and file transfer requires no manual intervention by the State. Automated transfer methods are more accurate than manual methods prone to human error. Xerox communicates electronically with the State multiple times a day to receive and transmit batch files and local TCP/IP traffic using an industry standard, electronically secure data connection with point-to-point data encryption.

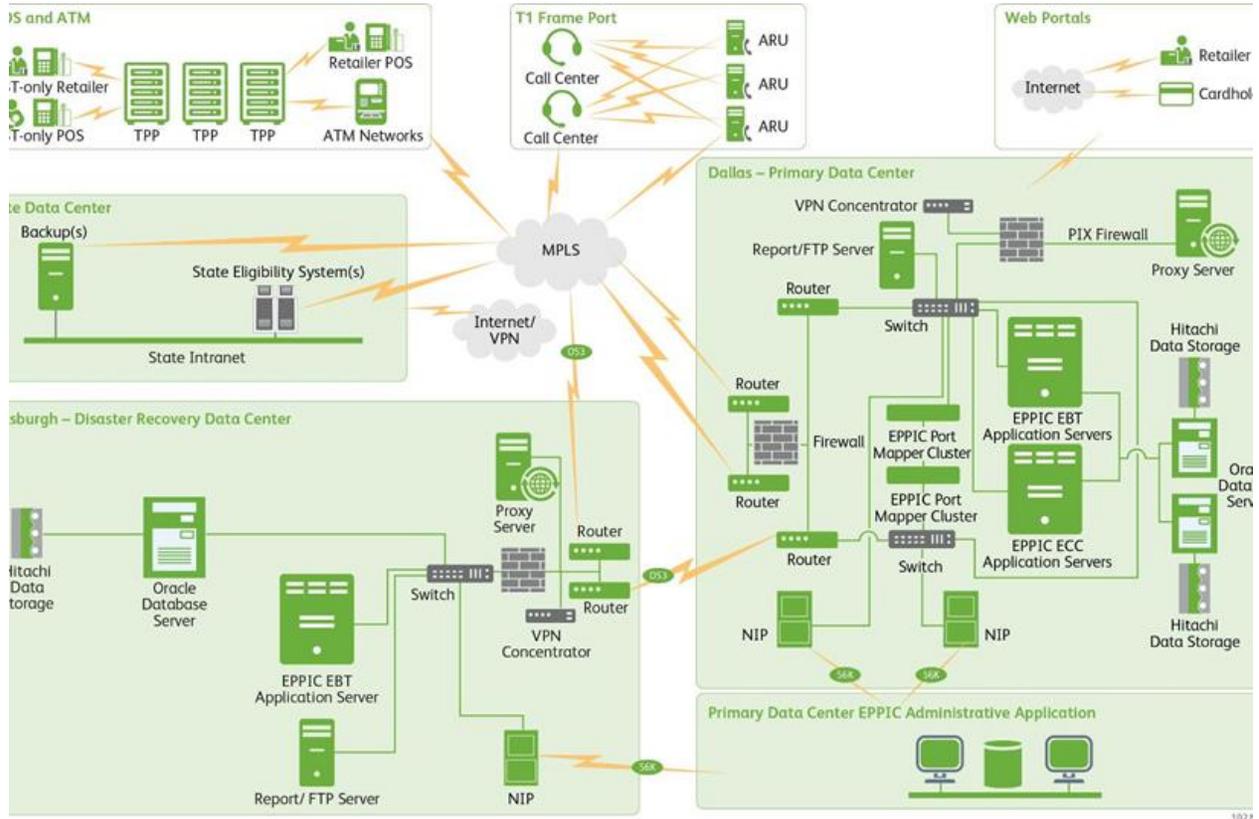
Xerox provides and maintains redundant communications links between the Xerox primary and backup facilities as well as redundant communication links between the Xerox primary and backup facilities and the State’s facility.

The transaction processing and call center networks will support the Vermont EBT system. Xerox establishes MPLS circuits to ensure redundancy, security, reliability, and sufficient bandwidth to meet the State’s needs.

Xerox leverages MPLS to efficiently transport transaction information between the State and EPPIC’s host processing system. MPLS is a high-performance telecommunications mechanism for carrying data that is used to speed up network traffic flow and simplify network management. This method provides an increase in bandwidth and performance to meet potential expanding data transmission need of EPPIC and Vermont. MPLS makes it easier to manage a network for quality of service as well.

The MPLS solution allows us to offer higher capacity backup circuits at all Xerox remote sites instead of the limited frame relay and ISDN redundant circuits currently in use in many state programs. MPLS provides a foundation for secure communication approaches, such as virtual private network (VPN) access for Web portals, or transmission and routing of encrypted transactions from POS devices. MPLS is installed in Xerox’s other programs with outstanding results.

Xerox Security Architecture



14.10 FISERV Card Production Processing Security

EBT cards are produced using blank plastic card stock purchased from an authorized vendor. Cards are received at Fiserv’s receiving dock where they are counted under dual control. The cards are labeled with identifying information and immediately transferred to the vault. The quality of cards received by Fiserv is tested to help ensure that the quality and physical dimensions meet the specifications of card production machines used by Fiserv. Cards are stored in a secured vault until they are retrieved for processing.

14.10.1 Fiserv Physical Security

All aspects of physical and production meet EBT security standards, which are the highest in the industry and conform to all applicable regulations. Cards will be produced and mailed from the Fiserv facility.

Security is continually emphasized by the presence of a security officer who reports directly to the president of Fiserv. Security is further emphasized by semi-annual, company-wide training sessions that address security responsibilities and adherence to Fiserv’s security policy. In

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

In addition, posters and notices informing employees of security policies are displayed at key locations throughout the facility.

Individuals hired by Fiserv are issued an ID badge that must be worn at all times. Employees use the ID badge to gain access to the facility as well as their work area. The ID badge includes an electronic interface for the card key system, employee photograph, and a color code, based on the area where the employee works. The ID badge must be swiped through an electronic keypad to enter the facility and secure areas within the facility. Access to employee entrances is electronically monitored and a detailed audit trail of activity is maintained. Employees must display their ID badges while in the facility.

A multi-level card key system controls access to Fiserv’s card production and PIN processing facilities, with access privileges granted according to an employee’s job function. A manager has been assigned responsibility for the administration of physical security at both the Stafford and Indianapolis facilities. Responsibilities of these individuals include issuing and deleting card keys, changing access when an employee’s job responsibilities change, and monitoring physical access. Human Resources is responsible for notifying the manager of physical security when a new employee is hired or an employee is transferred, leaves the company or is terminated.

A log is maintained that links each employee to his/her assigned ID badge. In addition, a record is maintained of lost ID badges. Employees who leave the company must surrender their ID badge to the security officer before departing the premises. Unissued or unused ID badges are the responsibility of the security manager and are inventoried in the security department under dual control. ID badges issued to employees that are not used during a one-week period are deactivated under dual control.

Visitors entering the building must sign in at the main desk in the lobby of the facility. Visitors must wear an identification badge while in the facility and the badge must be returned to the guard in the main lobby when the visitor leaves the facility. In addition, the guard is required to contact the person to be visited. The visitor is then escorted to his/her destination.

Access to the processing areas requires the use of a card key. As an added measure of security, access to the card vault room is protected by a biometric device that requires a personal identification number. A limited number of individuals are authorized to access the card vault room.

The loading dock area is surrounded by a twelve-foot fence and is fitted with inner and outer doors with an electronic mechanism to help ensure that both doors are never open simultaneously. Deliveries must be scheduled in advance, and drivers must provide appropriate identification.

14.10.2 Fiserv Personnel Security

The LAN administrator is responsible for logical access controls at Fiserv. User access to the system is granted based on the individual’s job responsibilities. Additions and changes to user profiles require the approval of a supervisor in the user’s department.

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

Fiserv has implemented stringent security features. Such features help ensure authentication of users, authorization to system resources (i.e., programs and data files), administration of access privileges and monitoring of user activity. A unique user ID and password is required for each user of the system, based on his/her job responsibilities. The password is not displayed on the screen when a user logs on to the system and is encrypted when transmitted over network lines.

Requests for user IDs originate from internal users and from Xerox’s project office. Project office users and Fiserv employees who request system access must complete an access request/change form, obtain management approval and forward the form to the LAN administrator.

Fiserv’s procedures require the LAN administrator to remove the access of terminated employees to the LAN. The procedure requires Human Resources to notify the LAN administrator of any employee who has been terminated.

Other security features include the use of a camera surveillance system that monitors the perimeter of the building, key areas in the facility and security personnel. The security system monitors the facility 24/7.

14.11 Addressing Security Deficiencies or Breaches

Should a security deficiency or breach be identified, the Xerox Project Manager immediately reports the issue to the Vermont project manager and follows the escalation procedures defined in the Xerox Incident Management Plan. The timing and method of escalation of issues varies based on its criticality. If it is critical, such as a security breach, the Xerox project manager immediately calls the Vermont project manager and follows up with written documentation. A non-critical deficiency, on the other hand, is reported in a regular project meeting and follows normal change management procedures to correct the problem.

Because of the nature of a security breach, Xerox senior management, Xerox legal division, and the Xerox security team are notified and provide policy and operational decisions to address the breach. Internal meetings are held to identify how the breach occurred and how to immediately halt it or recover from it. A more permanent strategy to prevent future breaches and update it once all information is known is formed. Depending on the occurrence, this strategy could include a redesign of components of the system architecture, redesign of aspects of the administrative terminal or Web portal functionality, or development or purchase of new fraud tools to better identify and prevent further intrusions. All along, Xerox is in constant communication with Vermont on Xerox’s immediate and longer term plans to prevent future intrusions. Providing frequent, open and honest communications with Vermont serves the best interests of all parties in properly addressing these situations should they ever occur.

14.12 Roles and Responsibilities

The roles and responsibilities of Xerox, the State, and any subcontractor(s) in maintaining security include important knowledge for each member of the project team. The information in this section helps ensure a coordinated approach to system security overall. Because of the

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

sensitive nature of security planning and management, the detail in this plan are necessarily limited. Further detail, if required, will be provided by the Xerox project Manager, Sylvia Mitchem.

14.12.1 Xerox and Subcontractors

The details provided in this section are based on the Xerox Information Security Policy that is cleared for external release.

Xerox business and technology managers are responsible for ensuring that all reasonable and necessary security controls are implemented within their environments to mitigate all unacceptable risk to their business. Business management choosing to outsource operations to other Xerox business or technology units, or external third-parties, retain overall responsibility for ensuring all reasonable and necessary controls are implemented and maintained to protect Xerox and client information, as well as meet contractual security requirements. All Xerox business and technology managers must ensure their units, at a minimum, meet all applicable requirements in the Xerox Information Security Policy.

- Workers will receive appropriate information security training regarding acceptable use of Xerox Systems and resources. Training will include the familiarization with and the location of policies, standards, and applicable procedures.
- Xerox will implement appropriate and reasonable IT security safeguards to protect Confidential Information in Xerox Systems. Xerox Systems will be configured with appropriate information security measures in a manner designed to protect Confidential Information from Security Threats.
- Each business unit will implement an appropriate access management process to ensure that access by Workers to Xerox Systems that transmit or store Confidential Information is appropriately managed, documented and reviewed. Workers will be provided with Minimum Necessary Access to a System for the purpose of performing appropriate business functions.
- Xerox Systems will be designed and configured for security and to protect confidential information from security threats.
- Xerox networks will be designed to maximize network availability and to ensure the security of Confidential Information and Systems from Security Threats.
- Vendor software will be used at Xerox in a manner that is consistent with applicable vendor licensing requirements and will be kept current with security patches. Internally developed software will be designed according to Xerox security standards and industry best practices; employing reasonable and appropriate safeguards to protect Confidential Information from Security Threats.
- Changes to production applications will be tested and implemented in observation of a documented change control procedure. This procedure will include appropriate

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

measures to ensure regular and emergency requests are reviewed, approved, and monitored according to Xerox security standards and industry best practices.

- Each business unit will develop Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP) for all critical Systems and operations, as appropriate. These plans will be regularly tested using Xerox or client (as applicable) standards.
- Xerox will perform routine checks to confirm that Systems are properly configured and patched to prevent exposing Confidential Information to Security Threats. This may be accomplished through the use of periodic vulnerability assessment scanning and targeted System penetration tests.
- Each business unit will perform internal assessments of its IT environments in the time and manner appropriate to the particular business unit, the Xerox Systems, the type and amount of Confidential Information involved and client requirements. Each business unit will be prepared to respond appropriately, as may be required, to an audit from either internal or external auditing entities.
- Security Incidents will be managed in order to mitigate and minimize exposure to Confidential Information stored or processed on Xerox Systems. Each business unit and location will respond to and report Security Incidents in accordance with Xerox Incident Reporting and Crisis management policies and, where applicable, location-specific procedures and client requirements.
- Xerox will take reasonable steps to select suppliers, vendors and contractors who maintain reasonable and appropriate IT security safeguards to protect Confidential Information and Systems.

15 Ceres Transfer & Implementation Contractor Security

15.1 Data Centers

Ciber Data Center Locations

- 650 Wilson Lane, Mechanicsburg, PA

All locations are secure access facilities, not open to the general public.

The main data center at 650 Wilson Lane is provided with multiple uninterruptable power supplies to ensure up- time in the event of a power outage.

15.2 Physical Environment

15.2.1 Power supply

- Redundant UPS system

15.2.2 Environmental Control

- Air-conditioned environment (Dual A/C units)
- Temperature and humidity control and monitoring

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

15.2.3 Physical Security

- Electronic Key Access
- Multiple-zone access control
- Lockable cabinets and racks
- Video Surveillance system monitors and records building entrance/exits and the data center

15.2.4 Fire Alarm systems

- Central Station Monitored

15.2.5 Types of Services

The following services are relevant to the MIS/EBT development and conversion system:

- Physical spaces for computers, servers, peripherals, networking, telecom and other equipment
- Server Hosting
- Backup and Recovery Solutions - Backups of servers and provide for safe storage and retrieval of all backup tapes and monitor for alarms. Backup and recovery services are provided by CommVault, which can be managed by designated Ciber CommVault Administrators.
- Power and cooling for computers, servers, peripherals, networking, telecom and other equipment
- Physical security for computers, servers, peripherals, networking, telecom and other equipment, as well as data storage devices such as disk and tape volumes
- Server Monitoring and Alerting - Monitoring and troubleshooting and customer support services, 7:30 AM-5 PM, M-F. Monitoring and back up call support off hours. Monitor system consoles for system errors and job failures.
- Remote job operation services
- Job scheduling services
- Server Antivirus and Multi-Tier Protection
- Server Maintenance, Patching and Updating
- Active Directory Services - Active Directory Services (ADS) is a manner to service all who login to a computer upon accessing the Ciber network. Authentication for the network is provided by AD. AD lets the computer know whether the requestor has the access to log on or not from any particular computer. ADS shares information to those who have the permissions to it. This includes printers. After a successful authentication, ADS can shield sensitive data from unauthorized access.

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

- SQL Administration & Support
- Server Configuration Support (DNS, DHCP, WINS)

15.2.6 Ciber Data Center Access

The Ciber Data Center is intended to enable systems administrators of the servers housed in a Data Center to be able to effectively manage their machines remotely and securely. All personnel must have proper authorization to obtain access to the Data Center.

Authorized individuals will have unassisted access to the Data Center 24 hours a day via key code entry panel.

15.2.7 Visitor Guidelines

Anyone who does not have an authorization code is considered a visitor. Visitors must be accompanied at all times by an authorized employee while in Ciber's Data Center.

15.2.8 Data Center Rules

- No food or drink is allowed within the Ciber Data Center.
- No hazardous materials are allowed within the Ciber Data Center.
- No cleaning supply is allowed within the Ciber Data Center without prior approval. This includes water.
- No cutting of any material (pipes, floor tiles etc...) shall be performed inside the Ciber Data Center unless special arrangements are made.
- Employees shall only access racks that contain equipment for which they are personally responsible.
- All persons must stay in their designated area.
- No person is to interfere with any equipment not managed by them.
- No person is to interfere with data center operations.
- All problems and/or concerns will be communicated to the Ciber Data Center staff.
- In the event of an emergency, notify Ciber Data Center staff immediately.
- All areas, including workstation, will be kept clean and organized.

15.2.9 Equipment

In order to enhance security and reduce the chance of disruptions, Ciber Data Center employees will deny access to anyone who intends to install or remove equipment without authorization.

The Ciber Data Center is intended to be a limited physical access location for servers. Systems administrators of machines, which are housed in the Ciber Data Center, must plan their servers as if they will only get physical access to them when it is necessary to perform hardware modifications or replacements.

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

Servers will be configured with secure access administrative tools to allow for remote maintenance. All machines in the Ciber Data Center must be rack mountable.

All new systems to the data center must undergo a security scan or audit prior to install. While the Ciber Data Center provides increased network security, it is still necessary to take care of host-based security policies. Hosts in the Ciber Data Center will be scanned regularly for vulnerabilities and those reports provided to the appropriate personnel.

All new systems and hardware to the Ciber Data Center will need to be coordinated and scheduled with the Ciber Data Center staff.

NO equipment may be placed outside of the designated rack.

NO objects may be placed on top of or next to a rack on the floor.

15.2.10 Portable Equipment

Portable equipment such as notebook computers should be fitted with locks designed for notebooks, and secured to a desk whenever possible.

- Unattended notebooks and portable equipment will be stored in a locked cabinet or room.
- Notebook computers will not be left in vehicles unless locked in the trunk out of view.
- Notebook computers will be protected from excessive heat and cold.
- Notebooks or portable devices will not be serviced or sent to surplus unless authorized by Ciber IT.
- All Ciber notebooks will have encrypted hard drives
- All Ciber notebooks will have McAfee Anti-Virus installed and monitored

15.2.11 Hardware/Software Maintenance & Upgrades of Production Equipment

- Authorized personnel may perform maintenance and/or repairs on equipment on an as-needed basis as approved by the Ciber Data Center Manager.

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

16 Information System Security Plan Completion Date

Enter the completion date of the plan.

17 Information System Security Plan Approval Date

Enter the date the system security plan was approved and indicate if the approval documentation is attached or on file

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

18 Appendix A Glossary

133DC	133 State Street Data Center
Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Agency - AHS	Agency of Human Services
AOT	Agency of Transportations
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticity	The quality or condition of being authentic, trustworthy, or genuine.
Authorizing Official	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Availability	Ensuring timely and reliable access to and use of information.
BDC	Barre Data Center
BGS	Building & General Services, Department of
Chief Information Officer	Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, executive orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.
Common Security Control	Security control that can be applied to one or more agency information systems and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Control	Process for controlling modifications to hardware, firmware, software, and documentation to ensure that the information system is protected against improper modifications before, during, and after system implementation.
COOP	Continuity of Operations Plan
Countermeasures	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

	safeguards.
DII	Department of Information & Innovation, State of Vermont
DIIDC	DII Data Centers
Information Owner	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Resources	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Policy	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Owner(or Program Manager)	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Information System Security Officer	Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for ensuring that the appropriate operational security posture is maintained for an information system or program.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Information Type	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, executive order, directive, policy, or regulation.
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
L3DC	Level 3 Data Center
Management Controls	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
National Security System	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

	by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
NLDC	National Life Data Center
Operational Controls	The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Privacy Impact Assessment	An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Protective Distribution System	Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information.
Record	Any written or recorded information, regardless of physical form or characteristics, which is produced or acquired in the course of agency business
Remote Access	Access by users (or information systems) communicating external to an information system security perimeter.
Remote Maintenance	Maintenance activities conducted by individuals communicating external to an information system security perimeter.
Risk	The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Risk Assessment	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.
Risk Management	The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.
Safeguards	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Security Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.
Security Control Baseline	The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.
Security Control Enhancements	Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Impact Analysis	The analysis conducted by an agency official, often during the continuous monitoring phase of the security certification and accreditation process, to determine the extent to which changes to the information system have affected the security posture of the system.
Security Label	Explicit or implicit marking of a data structure or output media associated with an information system representing the FIPS 199 security category, or distribution limitations or handling caveats of the information contained therein.
Security Objective	Confidentiality, integrity, or availability
Security Requirements	Requirements levied on an information system that are derived from laws, executive orders, directives, policies, instructions, regulations, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Senior Agency Information Security Officer	DII Official responsible for carrying out Statewide Information Security
SOV	State of Vermont
System Security Plan	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
System-specific Security Control	A security control for an information system that has not been designated as a common security control.
Technical Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
Threat	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Agent/Source	Either: (i) intent and method targeted at the intentional exploitation of a vulnerability; or (ii) a situation and method that may accidentally trigger a vulnerability.
Threat Assessment	Formal description and evaluation of threat to an information system.
Trusted Path	A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by untrusted software.
User	Individual or (system) process authorized to access an information system.
VDH	Vermont Department of Health
Visitor	An employee who does not work in the DIIDC; An employee who does not possess authorization to the DIIDC; A person who is not an employee of the State of Vermont.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Assessment	Formal description and evaluation of the vulnerabilities in an information system.

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

19 Appendix B: References

Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.

"NIST Guide to Information Technology Security Services", *National Institute of Standards and Technology* Special Publication 800-35, Oct. 2003. Web. 10 Oct 2011
 <<http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf> >

"SPIRIT Systems Documentation." *USDA FNS*. USDA, 06/09/2010. Web. 9 Aug 2010.
 <http://www.fns.usda.gov/apd/library/spirit_docs.htm >.

State of Vermont. Department of Information and Innovation. Policy Central. Montpelier:, 2011.
 Web. < http://dii.vermont.gov/Policy_Central>.

"WIC EBT Document Library" *USDA FNS*. USDA, 04/06/2010. Web. 9 Aug 2010.
 <http://www.fns.usda.gov/apd/library/wic_ebt_docs.htm >.

20 Appendix C: DII SOV Policy

- [Backup Policy](#) 
- [Change Control Policy](#) 
- [Electronic Messages Best Practice for All Public Agencies](#)  (2009)
- [Electronic Signature Guidelines](#) 
- [Electronic Signatures -- Best Practices](#) 
- [Electronic Signatures Best Practice for All Public Agencies](#)  (2010)
- [Incident Response Policy](#) 
- [Information Security Best Practice for All Public Agencies](#)  (2009)
- [Information Security Policy](#) 
- [Intrusion Detection and Prevention Policy](#) 
- [Malicious Software Protection](#) 
- [Minimum Security Standards for Application Development Policy](#) 
- [Physical Security for Computer Protection - Policy](#) 

VT WIC MIS/EBT Planning Project	Version: 3.1
Security Plan	Date: 7/14/14

- [Source Code Requirements for Business Applications](#) 
- [System/Service Password Policy](#) 
- [Third Party Network Connectivity](#) 
- [User Password Policy and Guidelines](#) 
- [Wireless Communications](#) 