E. Emergency Response and Disaster Recovery Plan

Describe the Vendor's proposed emergency response and disaster recovery plan, including a summary of how the plan addresses the following areas:

1. Essential operational functions and responsible staff members.
2. Plans to ensure critical functions and continuity of services to Providers and Enrollees will be met.
3. Staff training.
4. Contingency plans for covering essential operational functions in the event key staff are incapacitated or the primary workplace is unavailable.
5. Approach to maintaining data security during an event.
6. Communication methods with staff, Subcontractors, other key suppliers, and the Department when normal systems are unavailable; and
7. Testing plan.

Passport Highlights: Emergency Response and Disaster Recovery Plan

How We're Different	Why it Matters	Proof
20+ years of maintaining mission critical systems that serve the Commonwealth of Kentucky	• Our core MIS and all subsystems are already configured to meet the requirements of DMS and are currently functioning within the guidelines and specifications of the Commonwealth	• Passport has passed all DMS contract compliance audits that addressed Business Continuity/Disaster Recovery Plan (BC/DRP) capabilities and readiness
Ongoing independent third-party review of Emergency Response/Disaster Recovery Plan and supporting technologies	• Provides an unbiased approach to risk management • Recommendations facilitate the continuous quality improvement of our Emergency Response and Disaster Recovery Plan and Test Plan • Provides periodic actionable business and vendor business continuity risk mitigation recommendations • Ensures that all recovery systems and processes are maintained for peak performance and reliability	• Business Impact Analysis Report

Introduction

Kentuckians Serving Kentuckians

Planning for a disaster is of vital importance as Passport Health Plan's (Passport) management is responsible for the safeguarding of personnel, the protection of assets, the compliance with regulatory rules, regulations and purchasers, and of course, business continuity. Therefore, the Passport Business Continuity & Disaster Recovery Plan (BC/DRP) is a proactive measure to eliminate management's need to formulate and coordinate a plan of action when an emergency occurs. The BC/DRP ensures that necessary planning has already been done during the documentation phase prior to an emergency. All affected parties will have prior knowledge of their responsibilities during a disaster and consequent technology resumption efforts.

The ultimate purpose of the BC/DRP is to ensure that Passport can recover from a service interruption, of any nature or duration, in a timely and efficient manner, to emerge as a viable corporate entity able to effectively care for our members following the event. The plan and oversight include any functionality that has been sourced and provided by subcontractors, ensuring that key business functionality including, but not limited to, member and provider services, care management, claims adjudication, accounting, human resources and payroll can be recovered and resumed.

In addition to traditional sources of business interruption, Passport considers pandemic disasters in our emergency response and disaster recovery plan. Pandemics are defined as epidemics or outbreaks in humans of infectious diseases that can spread rapidly over large areas, possibly worldwide. There are distinct differences between pandemic planning and traditional business continuity planning. When developing business continuity plans, Passport typically considers the effect of various natural or man-made disasters that may differ in their severity. These disasters may or may not be predictable, but they are usually short in duration or limited in scope. Pandemic planning presents unique challenges to Passport. Unlike natural disasters, technical disasters, malicious acts, or terrorist events, the impact of a pandemic is much more difficult to determine because of the anticipated difference in scale and duration. The nature of the global economy virtually ensures that the effects of a pandemic event will be widespread and threaten not just a limited geographical region or area, but potentially every continent. In addition, while traditional disasters and disruptions normally have limited time durations, pandemics generally occur in multiple waves, each lasting two to three months. Consequently, no individual or organization is safe from the adverse effects that might result from a pandemic event. Due to these differences Passport recognizes the importance of a Pandemic Business Plan that focuses on addressing the unique challenges posed by a public health crisis. Passport's Pandemic Business Plan is included as part of our core Business Continuity Plan.

Describe the Vendor's proposed emergency response and disaster recovery plan, including a summary of how the plan addresses the following areas:

E.1. Essential operational functions and responsible staff members.

Passport is prepared to continue essential operational functions following an emergency or disaster through its BC/DRP. Passport's BC/DRP includes Information Technology (IT) disaster recovery planning involving the following operational environments and facility operations for primary locations and/or local office locations:

- Telecommute options for key staff
- Computing and information systems including the following:
  - Recovery of mission-critical applications: accounting, human resources and payroll
  - Recovery of email system and data
  - Recovery of Internet connectivity
  - Recovery of business/office applications and data
  - Recovery of remote-access capabilities and wide area network (WAN) connectivity

Passport's BC/DRP is designed to address all possible scenarios that could result in an interruption of services that support key and critical business functions. While we take great care in selecting and implementing technologies and services that have full redundancies, with no single point of system-fault failure, our BC/DRP has been designed to address service outages of any nature should they occur. These outages can be short term or long term and could include events such as the following:

- Failures of site-related component technology (e.g., server, router, switch)
- Vendor service failures or outages (e.g., Software as a Service [SaaS]/Infrastructure as a Service [IaaS] cloud services)
- Software-capability outages resulting from change deployment (e.g., deployment of new code resulting in the failure of a function)

In addition to outages and disaster scenarios that could occur at primary locations or local office locations, the Passport BC/DRP has been designed and tested to address worst-case scenarios that would render these locations inoperable or unavailable, causing an interruption that would last for as long as six (6) weeks. For purposes of this plan and policy, an emergency can include circumstances such as the following:

- Key staff are incapacitated
- The primary workplace(s) is unavailable
- The normal system(s) is unavailable

The scope of disaster considered in this plan is such that Passport's facility, key personnel, computing equipment, information systems and telecommunication systems cannot continue to function. This plan assumes that the facilities, data and telecommunication center at the Passport corporate office have experienced a disaster and all facilities, computing equipment, information systems, and telecommunication systems are out of service.

The Passport BC/DRP and recovery plan objectives and goals include the following:

- Providing recovery notification to Passport employees, providers and members as soon as possible
- Recovering essential functions within four (4) hours after a disruption
- Maintaining close communications with key personnel
- Returning to normal operations as soon as possible

This plan has been created to lead the restoration team through the tasks necessary to achieve the following:

- Provide facilities for operations for a limited number of staff
- Perform the following tasks to restore key IT and systems operations:
  - Ensure adequate, comparable hardware and software is available
  - Recover data, as needed, from backup and recovery systems
  - Reinstall software if necessary
  - Reestablish operating procedures
  - Ensure that critical application systems complete their cycles
- Restore Call Center/telephone operation

The BC/DRP's Recovery Time Objective (RTO) is set with duplicated replication running at fifteen (15) minute increments for core applications and four (4) hours for full recovery through the following:

- Redirecting calls coming through the business lines and 800 lines to the recovery site
- Failover of critical applications and systems to redundant data center facilities

This BC/DRP is designed to provide direction for managing and protecting the confidentiality, integrity and availability of Passport's information assets per regulatory requirements such as the Health Insurance Portability and Accountability Act (HIPAA). In accordance with Passport information security policies and procedures, this Information Security Program includes administrative, technical and physical safeguards to protect Passport information assets. Unauthorized modification, deletion or disclosure of information assets could compromise Passport's mission, violate individual privacy rights and possibly constitute a criminal act. Our chief operating officer has the key overarching responsibility for implementing the BC/DRP. Other responsible staff members include leadership of essential operational functions including those listed in **Exhibit E-1**:

Exhibit E-1: BC/DRP Responsible Staff Members and Responsibility

Primary Owner	Backup Owner if Primary is Unavailable	Responsibility
Chief Executive Officer	Chief Operating Officer	Overall Operations and public relations
Chief Operating Officer	Member Services Manager	**Disaster declaration, BC/DRP Plan execution.** Overall facility, IT, and Operations recovery

Primary Owner	Backup Owner if Primary is Unavailable	Responsibility
Chief Compliance Officer	Compliance Director	Overall CMS and DMS communications
Chief Financial Officer	Finance Director	Overall Finance recovery
Chief Medical Officer	VP Clinical Operations	Overall Pharmacy, Population Health, Quality, and Utilization Management recovery
Chief Marketing & Communications Officer	Marketing Director	Overall external communications and public relations
Management Information Systems Director	IT Operations Manager	Information Technology and Telecommunications recovery
	IT Security Officer	Maintains data security and integrity
Human Resources Director	HR Manager	Staff communications
Compliance Director	Compliance Manager	Subcontractor communications
Marketing Director	Marketing Controller	Media relations and communication
Provider Network Management Director	Provider Services Manager	Member/Provider portals recovery
Facilities Director	Facilities Coordinator	Facility recovery
Finance Director	Finance Controller	Finance systems recovery
Finance Controller	Senior Accountant	Finance systems recovery
Pharmacy Services Director	Pharmacy Services Manager	Pharmacy services recovery

E.2. Plans to ensure critical functions and continuity of services to Providers and Enrollees will be met.

Technology Plans

Passport oversees and operates a robust MIS. The BC/DRP plan ensures that the MIS and its subsystems remain fully operational in the event of an incident. The MIS and its subsystems are already configured to meet the needs of DMS and are currently functioning within the guidelines and specifications of the Commonwealth. Passport's MIS meets or exceeds all requirements of the Kentucky Managed Care Program, including member (services, third-party liability coverage, provider interface, reference, encounter/claims processing, financial and utilization/quality improvement. Our plan meets all applicable compliance and regulatory requirements as well as the requirements of our enterprise risk management program. For this section we will use the term Member in lieu of Enrollee.

In planning for business continuity and disaster recovery, certain instructions must be outlined, such as authority planning, RTOs, critical dependencies, manual workarounds, etc. Staff perform a variety of functions daily, including, but not limited to, the following:

- **Core Business Functions:** These are the functions directly related to delivery of services. They include, but may not be limited to, eligibility processing; claims receipt, adjudication and payment, along with associated banking functions; member and provider Call Center operations; utilization management (UM) functions; and provider data management.

- **General and Administrative Functions:** These functions include sales and marketing, human resources, finance and related control functions, compliance, facilities management and IT.
- **Operations:** Passport is responsible for operational continuity and will have overall authority to direct the activity of the departments covered in its BC/DRP. Passport's Operations team will work with other members of the Disaster Recover Committee to determine when functions will resume, the location, and any communication that should be shared with external parties (as related to business operations continuity).

In 2019, Passport completed a Business Impact and Information Technology Operational Analysis to identify critical business functions of the organization and the potential impact of a disruption of services. This analysis provided Passport with a categorization and prioritization of critical applications, identification of internal and external application dependencies, identification of the amount of time required to restore business functions as well as the acceptable amount of data loss, and the estimated resources necessary to meet the critical business recovery objectives.

The Application Operational Dependency Analysis grouped applications into three (3) key categories, in order of priority, in establishing continuity of services to providers and members. Please see our response to item four (4) of the RFP question for specific elements of the execution of the recovery procedure.

- **Tier 1—Mission Critical:** These applications have been identified as vital to business operations.
  - These are applications that are member-facing and critical to servicing members and providers, including the following:
    - Member and provider Contact Center(s)
    - Website(s) with provider directories
    - Member and provider portals
    - Tier 1 applications have been categorized with the highest priority to ensure member access to care.
- **Tier 1.5—IT Support for Tier 2 and Tier 3:** Recovery of these applications are required to operate the Tier 2 and Tier 3 applications and systems.
  - These are internal applications and critical IT systems, which includes the following:
    - Email
    - Fax service
    - Telephone connectivity
    - IT support systems
- **Tier 2—Business Vital:** These are the applications that support the operation of the business but are not immediately critical to core business processes.
  - These are applications that are not necessary for members to have access to care, but rather support business functions that do not have an immediate response for the member or provider, such as the following:
    - Claims systems
    - Financial systems

        - Grievances and appeals
        - Reporting systems
        - Records management systems
- **Tier 3—Business Non-Critical Utility Applications:** This category represents applications that support business operations but are not critical to the core business processes.
    - These are applications that are not necessary for members to have access to care, but rather support business functions that do not have an immediate response for the business, such as:
        - Intranet
        - Human resources systems
        - Accounting functions
        - Marketing systems

In 2020, Passport will conduct a gap analysis of the previous Business Impact and Information Technology Operational Analysis to ensure all changes to the organization are in line with the BC/DRP.

Monitoring Subcontractors

Passport carefully monitors the business continuity and disaster recovery capabilities of all subcontractors providing or contributing services that support critical Tier 1 through Tier 2 services. As part of Passport's delegation oversight responsibilities, we require all subcontractors to perform the following:

- Provide their updated BC/DRP annually
- Cooperate with on-site assessment of their BC/DRP capabilities, processes and supporting policies and procedures
- Submit Corrective Action Plans (CAPs) if gaps are identified or an unacceptable outage has occurred
- Address areas of risk
- Provide annual business continuity and failover testing outcome reports

For management and oversight of subcontractors, please reference **C.1 Subcontracts** response.

People Plans

In addition to the MIS solutions described, Passport has also established plans to address staffing needs to ensure that requirements for continuity of services to providers and members will be met. Passport will minimize risk to its employees at the workplace, communicate company-wide efforts and support of the workforce, and consider alternative work arrangements to support the stability and productivity of staff and services through the following process:

1. Key leaders within the organization determine when, how and who will make decisions regarding office closures.

2. Passport assesses the risk to employees of keeping any given office open. Passport identifies the essential business activities of the organization and prioritizes those positions considered critical to sustain service delivery.
3. Passport identifies how essential business activities can be maintained if large numbers of personnel are absent. Areas of focus include cross-training, telecommuting, etc.

Passport identifies core people/leaders within the organization and their backups (communicated across senior management). Please see Table E.1, under question 1 above for a full listing of titles and areas of responsibility.

1. Passport's leadership team works to identify how critical incident team members maintain a safe environment (e.g., use of masks) so that they are able to communicate member and provider issues.
2. Passport determines how to maintain the productivity of healthy employees with healthy families who are absent due to caregiving issues caused by mandatory school closings.
3. Passport also determines how to maintain the productivity of healthy employees who are absent due to government-authorized quarantine or movement restrictions.
4. Passport's corporate Human Resources department identifies existing resources that may be needed to support the workforce, including the Employee Assistance Program (EAP) and other benefit resources focused on building the resilience of employees.

E.3. Staff Training

Staff and key personnel training are essential to the successful implementation of a Business Continuity Planning Program. Passport's staff is trained on the contents of the plan, including the tiering of disasters, the prioritization of recovery for business functions, and the procedures taken in enacting our emergency plan. Staff are trained on the research and communications chains involved in disaster recovery functions.

The Passport Chief Operations Officer or their designee maintains the master copy of the BC/DRP in their electronic policy management system to promote business continuity and ensure all staff is aware of changes to our disaster response protocols. Training modules that include disaster scenarios are utilized for awareness activities. Training is required for all new hire employees and must be completed annually to reinforce the importance of business continuity and disaster recovery activities as outlined below.

As part of our overall plan, each department or critical function is required to participate by developing a sub-plan that details the specifics of their operations and what needs to be addressed, that ties directly into to the overall plan. Key roles and stakeholder responsibilities are also reviewed during this training. Contact information for key personnel is also shared. Since the Contact Center is our most critical function, all contact center staff are trained on how to respond in a disaster scenario depending on the severity of the disaster. Emergency meeting location preparedness is reviewed, and drills are performed to ensure staff and workforce can evacuate buildings and facilities in the event of a disaster. Staff are instructed to meet at designated safety zones outside and away from the building until such time that Passport leadership and or local emergency services officials deem it safe to return to the workplace. Employees are trained on all

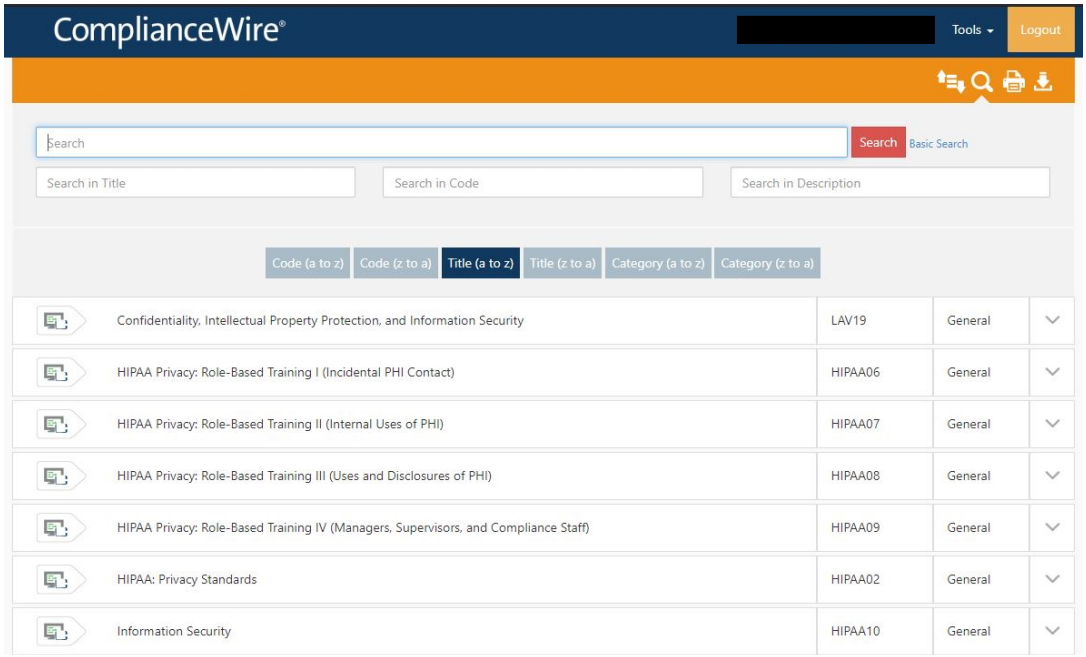
relevant emergency situations including building fire, severe weather, natural disaster, violent intruder and are provided step-by-step response guides and posters that continue to reinforce trainings as well as promote appropriate safe responses to emergencies. **Exhibit E-2: Emergency Action Safety Guide** below provides a sample of one of these many safety guides.

Exhibit E-2: Emergency Action Safety Guide

Passport carefully monitors staff training through our Compliance Management System (CMS), which captures when each employee or subcontractor accesses and completes each training module. Where appropriate, training modules include competency testing that assesses the employee's knowledge and comprehension of the training subject matter and requires a minimum score threshold to pass the test. In cases in which employees fail to achieve a passing score, they are given the ability to retake the test or the entire course. Our CMS provides a dashboard that reports on training compliance across multiple departments and domains. Employees failing to complete courses within the stipulated time frames automatically receive reminders when they are approaching training due dates, and when they have exceeded them. Notification and escalation rules are configured within our CMS to send notification to an employee's immediate supervisor if the employee is delinquent on completing a required training. Our CMS supports full version control management of all our training materials and maintains full traceability of all changes and approvals.

Please see **Exhibit E-3:** Compliance Management System (CMS) example below.

E-3: Compliance Management System (CMS) example



E.4. Contingency plans for covering essential operational functions in the event key staff are incapacitated or the primary workplace is unavailable.

Contingency Plans for Key Staff

If key staff are incapacitated and unable to fulfill their roles and/or responsibilities assigned to them as part of the BC/DRP, designated alternates will fulfill these roles and responsibilities. In order to cover essential operational functions, Passport conducts on a regular basis with department leaders the exercise of identifying essential/non-essential staff. As part of this exercise, the following outcomes are determined:

1. Identify employees working from home/remotely
2. Identify employees that are scheduled to be in the office
3. Identify primary and secondary points of contact for each department and notate whether those employees are working remotely or in the office

For details see the People Plan in Section 3 above.

Contingency Plans for Alternative Workplace Locations

Passport's two (2) primary business locations are in Louisville and Prestonsburg, Kentucky. In the event of an incident or disaster that would render either office unavailable, Passport's emergency operations procedures calls for employees to evacuate the building and immediately assemble at the designated congregation area away from the building. This evacuation and assembly plan assure the safety of our employees, while creating space to allow emergency personnel to access the locations.

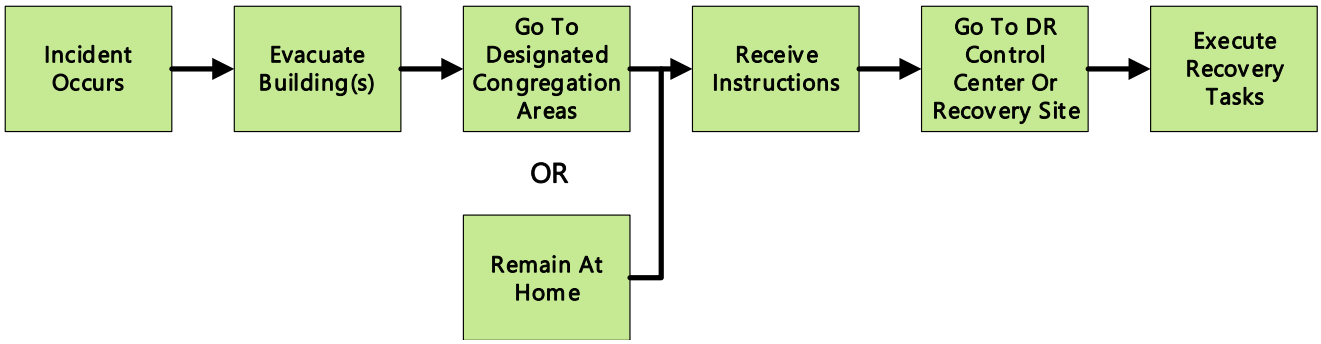
In the event Passport primary locations are unavailable all Passport staff have the ability to securely:

1. Work from home/remotely
2. Work from temporary alternative locations
3. Work in any WIFI enabled location

Recovery Procedures

The sequence of events shown in **Exhibit E-4** is to be followed prior to implementing any assigned disaster recovery responsibilities. This procedure is necessary to ensure that all Passport employees, and key personnel, are accounted for after the onset of the emergency condition. The primary responsibility is to move to the congregation area or remain at home to receive additional recovery instructions and information.

Exhibit E-4: Initial Sequence of Events



Return to Normal Operations: Reconstruction Plans for Re-Recovery at Original Location

The recovery will depend on the severity of the issue and its impact to the business. For example, recovering the business from a total loss resulting from a natural disaster will require different strategies and procedures than a less severe event like a systems outage.

The recovery process will always follow this methodology once the disaster scenario ends:

1. Full evaluation of damage or degradation
2. A mitigation plan is created and executed on to address damage or degradation
3. After greenlighting restoration, the systems will be returned to normal state
4. After action review is then performed

Information Technology (IT) is empowered to monitor the process and implement Passport's post-disaster recovery procedures. The plan for post-disaster recovery and reconstruction should have, as part of its

policy objectives concerning business recovery, not just the objective of restoring normal business activity but that of making it more resistant to such disruptions should disaster strike again. Determining exactly which measures are appropriate and effective in accomplishing this mission is an essential function of the planning process.

After Action Review (AAR)

An after-action review (AAR) is a qualitative review of actions taken to respond to an emergency as a means of identifying best practices, gaps and lessons learned. Following an emergency response to disaster scenario, an AAR seeks to identify what worked well or not and how these practices can be maintained, improved, institutionalized and shared with relevant stakeholders.

Various types of damage assessments performed during the early recovery period provide opportunities to assess the effectiveness of any previous mitigation efforts.

Implementing strategies requires the elaboration of priorities, and the establishment of priorities must be based on clear criteria. Risk assessment is a critical factor in establishing those criteria because considerations related to protection of employees and critical facilities will inevitably drive these priorities.

Hazard mitigation is an implicit function of all other objectives of the plan for post-disaster recovery and reconstruction. Nonetheless, mitigation needs to be highlighted in the plan in order to achieve the visibility and priority it deserves. As a policy objective, mitigation should be seen as posing the following two (2) sets of opportunities that deserve distinct treatment:

1. Those pursued during the pre-disaster period and programmed into daily operational activities and budgets on an ongoing basis
2. Those created as an immediate result of a natural disaster and that must be acted upon in a timely manner during the recovery and long-term reconstruction periods.

Finally, hazard mitigation works best as a policy objective of local planning when it is completely integrated into the comprehensive plan, such that it becomes a normal assumption behind all daily planning activities.

E.5. Approach to maintaining data security during an event.

Passport recognizes the importance of keeping all information confidential and has made data security a key component of our policies and procedures, including our BC/DRP. Due to the nature of Passport's BC/DRP configuration, privacy and security standards are continually in force and never diminished. Passport has a multifaceted approach to security, incorporating physical, application, Internet, electronic, administrative and clinical transaction security. This includes many tools and processes to ensure proper oversight is maintained. The Information Security Program includes the following high-level capabilities:

- Network intrusion detection appliances on both the perimeter and internal local area network (LAN), monitored 24/7
- Intrusion detection, log correlation and system event monitoring
- Data Loss Prevention (DLP) technology that enforces policy restrictions on data at rest and in motion

- Protocol filtering on network ingress/egress access points
- User credential management and access oversight
- Data encryption and virtual private network (VPN) mandates
- Transport Layer Security (TLS)/Secure Sockets Layer (SSL) encryption for appropriate Internet and VPN traffic
- Continuous auditing of information systems via internal and third-party examiners
- Comprehensive system hardening through configuration restrictions and patch management implementation
- Ongoing security awareness and compliance training for all Passport employees

Uninterruptible power supply (UPS) backup and on-site generators are primed, fueled and tested monthly. Electrical, smoke and fire alarms are monitored 24/7 and configured to alert personnel in the event of an incident. All system health and temperature readings, as well as physical and environmental controls, are configured to alert as necessary and are monitored continuously.

Passport uses various methods to ensure the maintenance of data security on a regular basis. These measures will continue to provide data security during an event. One such method is Passport's use of access profiles to restrict access to data. These profiles are typically segmented by job class, ensuring that workforce members can successfully perform duties while reducing the chances of inappropriate exposure of protected health information (PHI). Access is granted through a rigorous process that requires management approval. A user account is disabled after a predetermined number of failed access attempts, and system administrators then must validate the user's identity before unlocking the account.

In addition, Passport promotes physical security by maintaining exhaustive security practices related to our facilities and ensuring that all staff are trained as new hires and then annually on these practices. Our physical security practices include the following:

- Remote cameras continually survey the outside of the building.
- Each employee is issued a photo identification badge, and badge information is maintained in a computer system that is updated in real time to restrict access.
- The security system records all activity for all identification cards.
- Physical access to all data centers is severely restricted to authorized employees or escorted guests only.
- Guest passes are restricted, and all guests must be verified and accompanied by an employee.
- All computer screens are to be locked when employees are away from their desks.
- All portable PCs and mobile devices are locked in a desk or secure area or taken home when employees leave for the day.
- All sensitive documents are locked in secure desk drawers or cabinets and not left on desks or printers.

The MIS captures and stores a comprehensive set of data about our members and providers. We maintain several years of data and are constantly creating new and innovative ways to collect and use data. Our goal

is to continuously monitor, assess, report and improve the data we collect and analyze—which allows us to make better-informed decisions for our members. This improves member care and optimizes cost-effectiveness. For 22 years, Passport has successfully and securely exchanged data with our business partners/subcontractors and DMS. We consider our secure interfaces one of our strengths and continue to search for innovative and automated ways to securely transfer data when needed.

Passport focuses on stringent protocols and supports multiple HIPAA-compliant file formats—and requires the same from our trading partners. Data exchanges between DMS, providers and vendors occur through dedicated point-to-point (P2P) connectivity, secure VPNs or encrypted SSL connections over the Internet. Passport uses the MoveIT DMZ and MoveIT Central products to perform job scheduling, automation, status monitoring, exception alerting, logging and reporting of secure file transfers inside the organization and with other organizations. This software suite allows for extensive file transfer automation capabilities to support business functions 24/7.

Passport routinely self-audits performance, security and operational controls and participates in DMS and regulatory audit processes annually. Requests for access or documentation are processed within prescribed time frames, and any subsequent follow-up or suggested actions will be agreed upon and executed.

System Redundancies

Data Centers

Passport has system redundancies at multiple sites with the ability to ramp up as needed in the event of an outage and has the capacity to perform operational functions at multiple sites across the country.

Our primary and backup data centers are approximately 1,100 miles apart. This distance and geographic diversity greatly reduce the possibility of both sites being impacted by a single natural disaster or event. In the current configuration, the primary data center for Passport is Flexential-Louisville, with Flexential-Denver as the backup site. The goal of the network design is to be fully active-passive, meaning that both Louisville and Denver maintain equivalent network, compute and storage systems in a high-availability configuration. Since Louisville is the primary worksite location for Passport, equivalent network connectivity shall be maintained from it to both the Louisville and Denver data centers. Dedicated connectivity is established between the Louisville and Denver data centers to support the services required to deliver the desired state of availability—simple replication or complete application and system mobility. The passive (failover) site serves as a backup that is ready to take over as soon as the active (primary) site gets disconnected or is unable to serve.

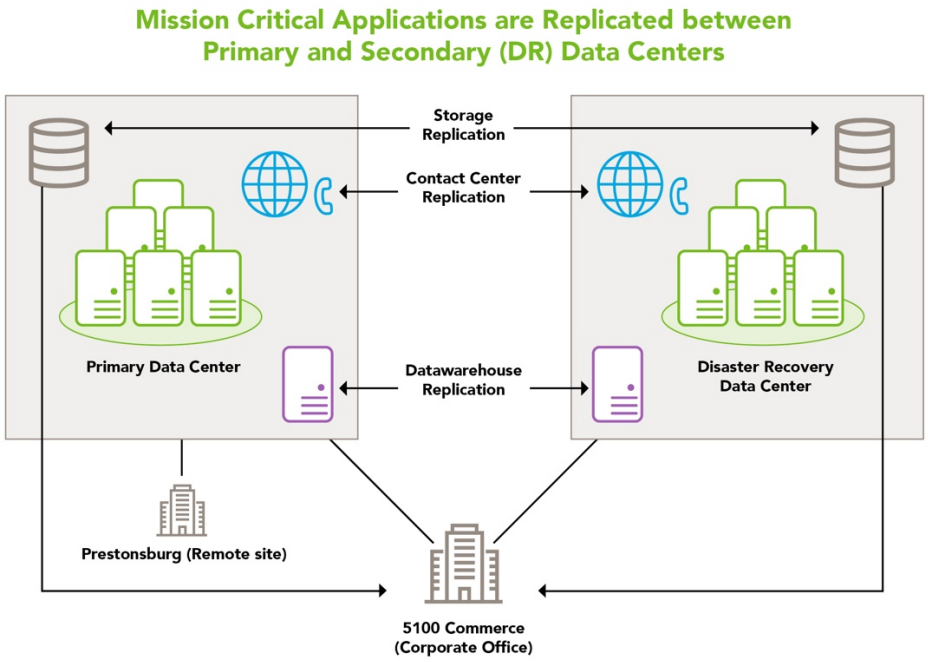
Our Flexential-Louisville primary and Flexential-Denver backup sites maintain the highest level of annual security and operational compliance and certifications, which includes the following:

- PCI DSS (See **Attachment E-1_2019 PCI DSS AOC**)
- HIPAA Compliant
- HITRUST CSF Certified (see **Attachment 60.E-2_Flexential-2018-HITRUST Certificate** and **Attachment E-3_Flexential-2019-HITRUST Interim Letter**)
- SOC 1, 2, and 3 Type 2

- ISO 27001 (see **Attachment E-4_Flexential-2019-CORP ISO 27001 Re-Issue Certificate**)
- NIST 800-53
- EU-U.S. Privacy Shield Framework
- FISMA High Suspicious Activity Report (SAR) (see **Attachment E-5_Flexential-2019-FISMA High SAR**)
- ITAR

Passport's Application Operational Dependency Analysis grouped applications into three (3) key categories as described previously to ensure critical functions and continuity of services to providers and members will be maintained in the event of an incident or disaster. Many of the Tier 1 applications are web-based SaaS; however, there are several mission-critical applications based in the Flexential-Louisville data center. The operational and backup plan for these applications and systems are significant. From a technical perspective, the high-availability environment within Flexential will ensure continued operation and availability. If Flexential-Louisville becomes unavailable, applications and systems are backed up and replicated to Flexential-Denver. **Exhibit E-5** on the following page presents an overview of our redundant data centers.

Exhibit E-5: High-Level Enterprise Network Architecture



For restoration of servers, Passport uses EMC, Zerto and VMware solutions:

- The primary data center is in Louisville, Kentucky
- The data center recovery site is in Aurora (Denver), Colorado

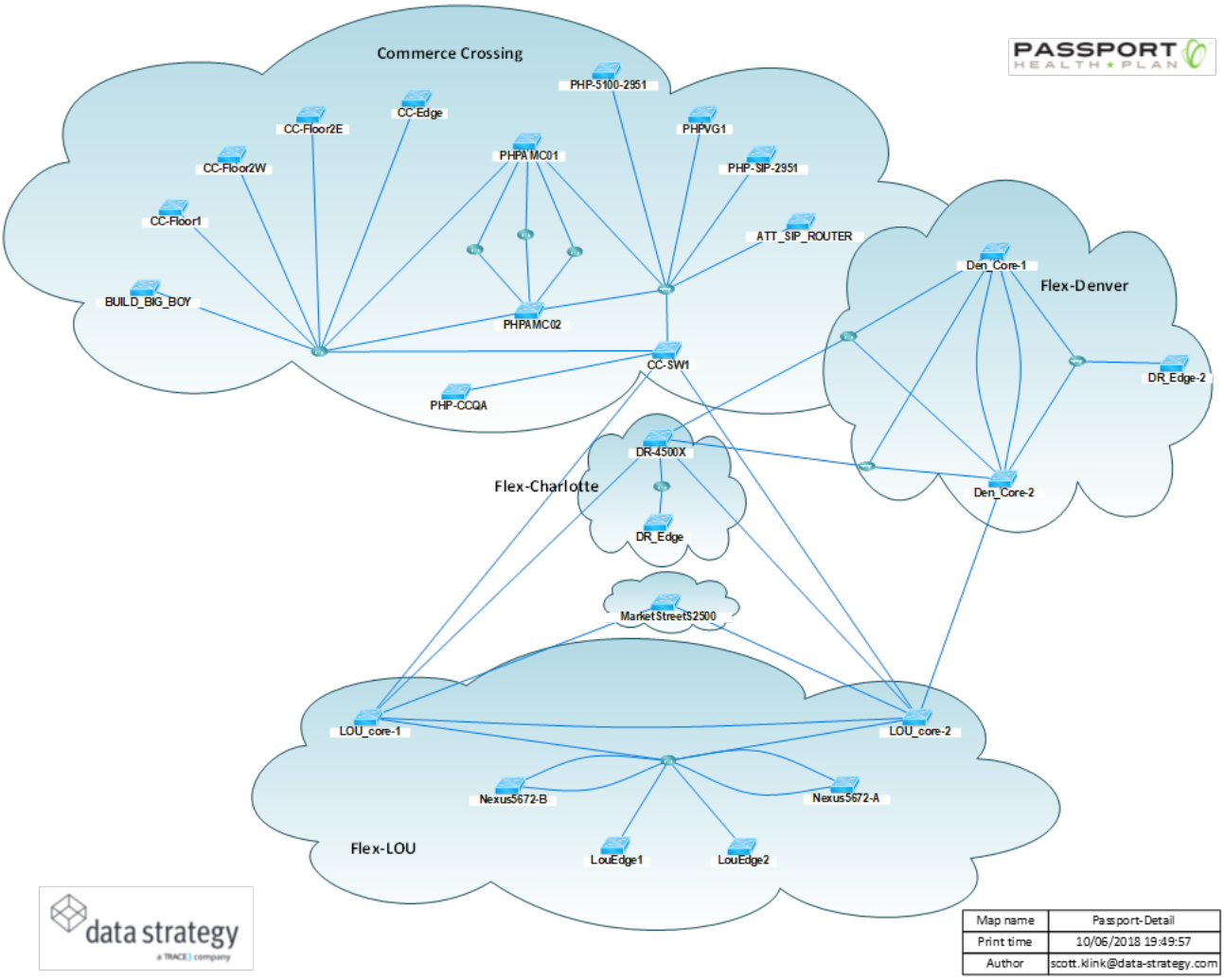
The following is a summary of the locations and interconnectivity for the Passport network:

- Commerce Crossing—main office
- Two primary data centers—planned for an active/passive operational state
  - Active—Flexential Louisville

- Passive—Flexential Denver
  - Passport plans to operate workloads from the Denver data center continuously
  - Two satellite offices
- Prestonsburg, Kentucky, interconnected via a layer-two P2P connection

Exhibit E-6 shows the detailed interconnectivity of all Passport locations and equipment.

Exhibit E-6: Passport Location and Equipment Interconnectivity Diagram



Voice Carrier Services Connectivity and Gateway Location

Telephone services to Passport are delivered on Session-Initiated Protocol (SIP) to a Cisco Unified Communications voice gateway currently operating at the Passport corporate office. The Cisco Unified Communications Systems and Contact Center servers and software are redundant and operating at Flexential-Louisville.

Call Center agents have the capability to work remotely—the Unified Contact Center Express agent can operate with a Cisco softphone endpoint, effectively enabling agents to work anywhere that supports secure connectivity to Passport network services.

E.6. Communication methods with staff, Subcontractors, other key suppliers, and the Department when normal systems are unavailable.

The chief operating officer or his/her designated alternate will have sole responsibility for declaring a disaster and will ensure that the disaster notification procedure is initiated.

The chief operating officer will identify a disaster recovery control center location and notify each individual identified in the contact list. Each responsible leader will notify his/her managers and their staff.

If normal systems (i.e., email, Internet connectivity) are not available, we will use a pre-populated contact list of key personnel's mobile phones, landlines, personal email addresses and preferred personal communication methods (i.e., social media and instant messaging).

Disaster Calling Procedure

The initiator of a disaster notification will first call police, fire or other emergency services as appropriate and will then attempt to call an individual in the roles identified. The first individual contacted is responsible for calling the members in his/her area and notifying the initiator of the results of these efforts. Each member on the list is responsible for notifying managers and staff members of his/her respective department. If the initiator cannot reach a particular individual on the list, he/she will continue to attempt to call additional people. Each person on the list will report results back to the initiator.

Notification to Members and Providers

The Marketing and Communications department is responsible for notifying Passport providers and members regarding the occurrence of a disaster event and operation in disaster mode. This department is also responsible for providing updates as well as notification when normal operation mode is reestablished.

Notification to Subcontractors

The chief operations officer or his/her alternate will communicate with each of our subcontractors in order of priority/criticality, following the Subcontractor Notification Plan. This plan includes a prioritized list of key personnel and leadership, as well as primary and secondary contact information including contact method (phone, email, text message and/or internal business units with direct contact).

Notification to Federal and State Regulators

The chief compliance officer is responsible for notifying the appropriate federal and state agencies regarding the occurrence of a disaster and operation in disaster mode. Key staff at each agency will be contacted based on a notification tree that includes primary and secondary contacts and methods (phone, email, text

message). The chief compliance officer is also responsible for providing updates as well as notification when normal operation mode is reestablished to stakeholders including, but not limited to, the following:

- Centers for Medicare and Medicaid Services
- Kentucky DMS
- Kentucky Department of Insurance (DOI)

E.7. Testing plan

On an annual basis, the Passport Information Technology (IT) department investigates and tests the overall recovery and backup operations process, including the Information Systems and Telecommunications components of the plan. Results of this investigation and testing are reported to leadership and the plan is updated accordingly. The plan is reviewed, updated and distributed to stakeholders at minimum on an annual basis or after substantial system or business changes. All subcontractors are contractually required to participate in the testing and evaluated jointly and independently for failure points or best practices that can be shared. This includes our hosting data centers.

Background

In accordance with State and Federal regulatory requirements, Passport has developed and implemented a comprehensive Business Continuity and Disaster Recovery (e.g., BC/DRP) testing plan. As part of our annual testing and due diligence, testing procedures (or BC/DRP drills) are conducted in core business areas to test the effectiveness of the DR/BCP.

This goal of this testing on the continuity of critical/core business services is to ensure they would not be interrupted, or that the appropriate mitigation plans are in place to address disruptions in a timely manner. During the testing, IT system failover is evaluated, and interviews are conducted with core business areas to ensure they would easily be able to talk through BC/DRP process and the related procedures.

Testing Scope and Methodology

The scope of this type of test includes a disaster scenario affecting the Passport corporate office and data center both located (separately) in Louisville, KY. As a part of the testing, the BC/DRP team reviews the following: Evacuation procedures and drills, notification procedures, determining how data privacy and security would be maintained during the testing, and operating the business in a timely fashion from a remote location. The BC/DRP team consists of key members from the Information Technology, IT Security, and Compliance teams.

The methodology for this testing is a question and answer style interview, following the reading of the scenario, which the affected business team receives for the first time during the testing process. The questions are not shared prior to the test, since the goal is to make the testing format as real as possible. The BC/DRP team also collects documentation from the affected business team (being tested) regarding their departmental Disaster Recovery and Business Continuity plans to confirm compatibility with the core DR/BCPs.

In addition to the core business area testing, the IT team conducts an annual failover test to a full alternate data center. The goal of this testing is to evaluate the IT team's ability to resume business operations using an alternate data center if the primary data center becomes unavailable. The performance of the drill is measured by the ability to meet two primary requirements: Recovery Time Objective (RTO) and Recovery Point Objective (RPO). The baseline metrics for meeting these RTO/RPO requirements are documented as part of the DR/BCP.

During alternate-site failover testing, the IT team will maintain and update a DR failover checklist. Each checklist begins with an inventory of networking and systems equipment, services and applications. Regarding the networking, key infrastructure—such as routers, switches, security and optimization devices—are included in the drills to ensure that recovery or repair efforts produce functional networks, systems and core services. This testing also considers carrier-level access and equipment, and media and system failures. Each core business area will have a delegate selected prior to the technical failover testing phase. It will be the responsibility of the business delegate to communicate throughout the testing process and report on how his/her team's services were impacted (if at all) during the failover.

Testing Outcome

Once each phase of the testing has completed, a post-mortem review will be conducted internally by the BC/DRP team. This meeting will consist of the BC/DRP team (e.g., IT, Security, and Compliance), but may also involve other areas of the business (depending on the scope of the test). A report will be produced outlining the testing process and results; and documenting the findings / recommendations for future actions.

As a part of this final review process, results of the test will be compared against pre-established baseline metrics (i.e., RTO/RPO) to determine what actions and/or recommendations will be needed to improve the BC/DR process. These results will be documented in the testing outcome final report in a pass/fail manner with comments included where appropriate.

Passport will comply with all requirements contained in Attachment C, Medicaid Managed Care Contract. Particularly relevant for this section are the CHFS Security Requirements of Appendix Q. The Appendix contains suggested Disaster Recovery drill suggestions. Passport will evaluate each of the suggested drills and, where not already included in Passport's testing, will incorporate them.

Conclusion

Passport's Emergency Response/Disaster Recovery plan serves as a comprehensive resource that is implemented to assure that all critical personnel, systems and processes are resilient and continue to serve Kentuckian's in the event of an emergency. As our overall Emergency Response and Disaster Recovery Plans are available at our operational sites and those of our subcontractors, we invite DMS on-site to review them at length prior to the award of the contract. We appreciate the opportunity to present our BC/DRP and answer DMS's specific questions and look forward to continuing our 22 years of uninterrupted service to the Commonwealth.

Passport has been honored to serve the Kentucky Medicaid and foster care populations for 22 years and will continue to comply with all provisions of the Medicaid Managed Care Contract and Appendices (including Kentucky SKY) as we continue to serve them in the future.