HRO TODAY ASSOCIATION *HR (Buyer) Resource Toolkit*

Business Continuity Plan (Escalation Protocols)

Business Continuity Plan

Prepared for: Insert Company Names and Program Title

Issue Date/Revision Date: XX/XX/XXXX

Client Signature(s):

____

Document Storage Location:

____

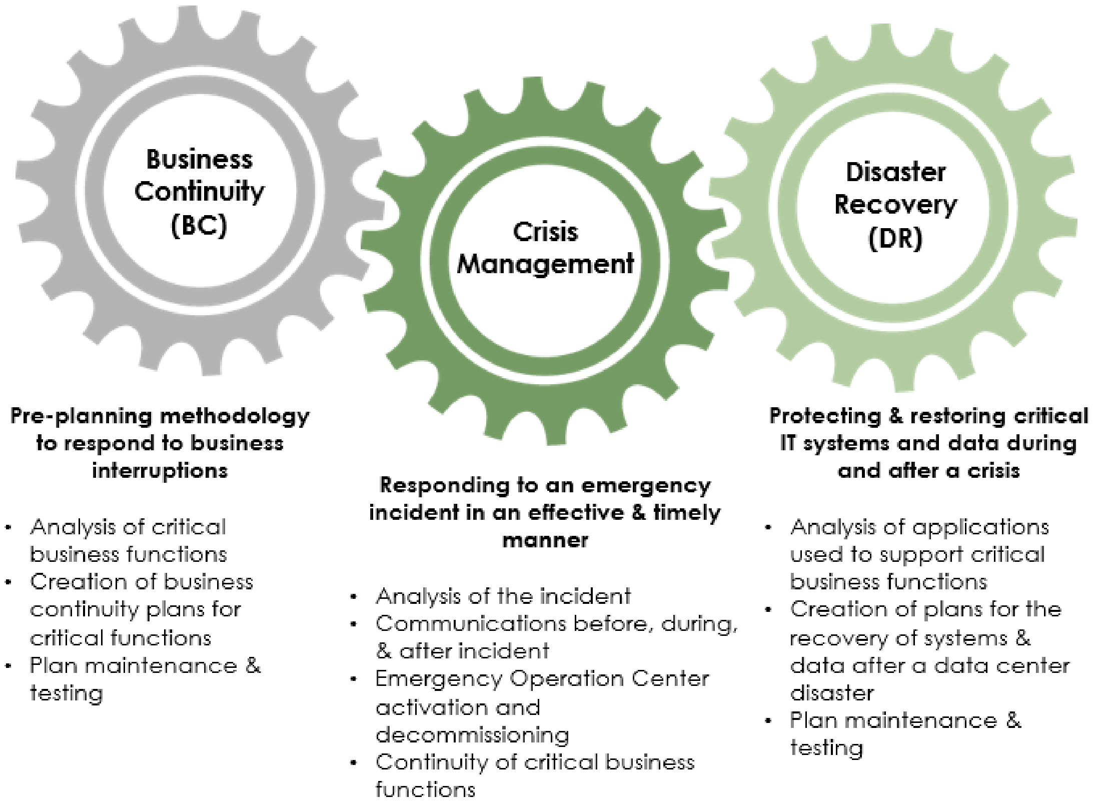
Contents

A focus on business continuity is a key component of the risk management program. Being prepared to respond to situations such as natural disasters, safety, and security concerns, and changing business conditions quickly and effectively is critical to the health and safety of employees, the interests of shareholders and customers, and the viability of the Company. Suppliers should utilize a variety of scalable solutions and strategies to both ensure employee health and safety and enable the partnership to continue critical business functions after experiencing virtually any type of disruption.

BUSINESS CONTINUITY

Your business partner should recognize that unplanned business interruptions resulting from natural disasters, power outages, fires, civil unrest, disease outbreaks, and other natural and man-made disasters can and do occur. Not only is preparedness for these situations critical to the interests of customers, but it is also equally important to the health and safety of employees. To that end, business continuity planning should be incorporated into the overall business strategy.

The HR Services and/or Technology Provider should employ a proactive, all-hazards approach to preparing for business disruptions. This multi-pronged and flexible strategy allows them to respond and address the severity and scope of the threat. There needs to be an established emergency communication plan, and an integration of business continuity plans between provider and customer. The following is one example of capabilities, and this approach includes three functions: *Business Continuity, Crisis Management and Disaster Recovery.*



Pre-planning methodology to respond to business interruptions

- Analysis of critical business functions
- Creation of business continuity plans for critical functions
- Plan maintenance & testing

Responding to an emergency incident in an effective & timely manner

- Analysis of the incident
- Communications before, during, & after incident
- Emergency Operation Center activation and decommissioning
- Continuity of critical business functions

Protecting & restoring critical IT systems and data during and after a crisis

- Analysis of applications used to support critical business functions
- Creation of plans for the recovery of systems & data after a data center disaster
- Plan maintenance & testing

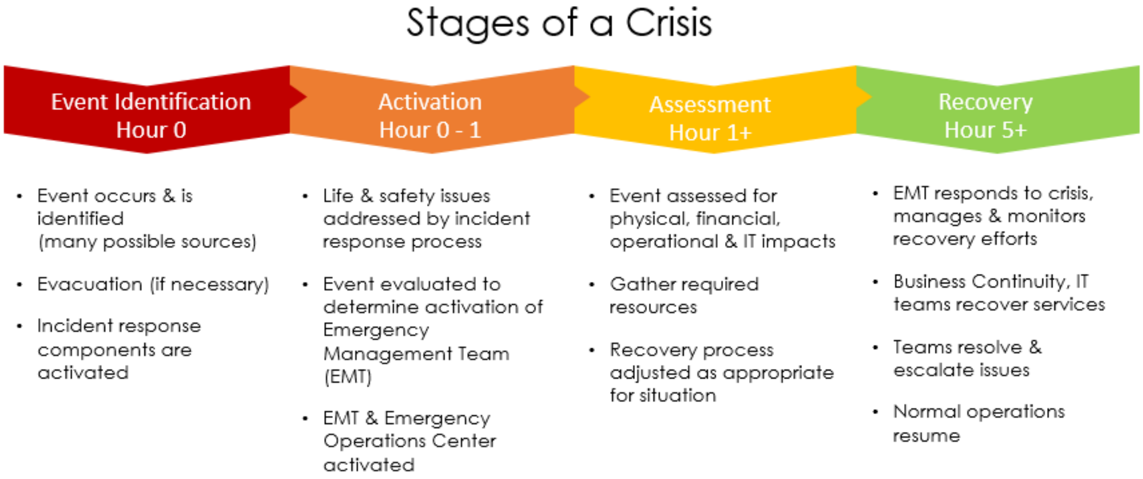
Crisis Response Capabilities

Providers ability to develop and effectively utilize a variety of scalable solutions enables continued critical business functions after experiencing virtually any type of disruption. The ultimate success of the strategy is based on the following basic components:

- **Global Incident Monitoring**: Provider invests in technological resources that enable them to globally track and monitor crisis events that may affect employees, facilities, and operations. Having first-hand knowledge of the proximity of operations and/or employees to a crisis event allows a response in an efficient and effective manner.
- **Communications**: A comprehensive communications protocol (including on-demand automated voice calling, bulk texting and mass emailing) that leverages a variety of methods to maintain communications with employees, clients, and vendors/suppliers before, during, and after a crisis event.
- **Emergency Management Team**: This team of decision-making representatives from across the Provider business and service sectors are empowered to make strategic decisions in response to critical events that affect their employees and facilities.

- **Continuity of Operations**: Based on the depth and breadth of the providers reach or network, as well as a single front-office database, Provider can replicate business operations to alternative sites if one becomes inoperable.
- **Emergency Operations Center**: A dedicated facility is available to support field operations, clients, and employees in the wake of a crisis event.
- **Uninterrupted Power Supply:** In the event of a power outage, a UPS System (uninterrupted power supply) automatically activates for Providers Headquarter operations. This failover operates as our generator warms up and once up to full speed, the generator powers data center, life systems (e.g., emergency lighting, elevator), telephony rooms, and security systems.
- **IT Disaster Recovery:** Provider is contracted with a reputable global leader in IT data center restoration. Within 24 hours of an IT disaster declaration, the vendor ensures availability of the equipment necessary to run Provider's critical IT systems from a remote location.

Response to a crisis event follows the stages identified in the graphic below:



Stages of a Crisis

Event Identification
Hour 0

- Event occurs & is identified (many possible sources)
- Evacuation (if necessary)
- Incident response components are activated

Activation
Hour 0 - 1

- Life & safety issues addressed by incident response process
- Event evaluated to determine activation of Emergency Management Team (EMT)
- EMT & Emergency Operations Center activated

Assessment
Hour 1+

- Event assessed for physical, financial, operational & IT impacts
- Gather required resources
- Recovery process adjusted as appropriate for situation

Recovery
Hour 5+

- EMT responds to crisis, manages & monitors recovery efforts
- Business Continuity, IT teams recover services
- Teams resolve & escalate issues
- Normal operations resume

Pandemic Planning

Pandemic events should also be included in Supplier's overall business continuity plan. Due to the unique response requirements of pandemic events, the Provider should have developed tools and resources specific to these situations. For example,

- Guidelines and processes that cover everything from infection control measures to communications, education, and travel safety.
- Policies related to sick leave, pay continuance, exclusion of ill employees from the workplace, and telecommuting.

Business Continuity and Disaster Recovery Exercises/Testing

To ensure maximum readiness, emergency response and recovery procedures should be regularly audited and tested as part of a continuous improvement process. Providers should exercise their Business Continuity Plan and Emergency Management Team responses on an annual basis. BC exercises may focus on operational impairments and generally include representatives from Security, Operations, Finance, Law, Risk Management, Human Resources, Marketing, Communications, and IT. IT Disaster Recovery exercises should test plans for potential impairments of data and be conducted semi-annually. Provider should be able to provide dates exercises/testing was completed and results. Updates to the plans, as appropriate based on the results of these exercises, should be made accordingly.

Third-Party Systems

If the Provider maintains contractual agreements with vendors in support of the business that will be conducted within the scope of work they have been assigned through the partnership they should confirm that they review their vendors and disclose the process used to do so. Where available, they should at least annually review each of their vendors <independent service auditor’s report> maintained in their system, to ensure the sustainability of the design, and operating effectiveness of their controls. These reports can be reviewed and prepared in accordance with the AICPA SSAE No. 16 and IAASB ISAE 3402 standards. Specifically, they verify that the independent auditor has not noted any material exceptions to the design and operating effectiveness of each vendor’s prescribed controls.

Provider Business Continuity in Action

Providers should be able to provide examples of how their business continuity planning program has proven itself over the last several years. Inevitably they have experienced disaster events, such as local and regional power outages that affected their operations, as well as natural disasters such as hurricanes and earthquakes that affected office and/or satellite operations. In situations like these, they should be able to provide examples of their ability to immediately mobilize an Emergency Management Team and implement business continuity plans, enabling them to get critical business operations up and running within a reasonable or agreed upon timeframe. Other examples include:

- 2020 COVID-19 (Coronavirus)
- 2020 Hurricanes Zeta, Sally, Laura, Marco, Douglas,
- 2020 California-Washington-Oregon wildfires and Australia brushfires
- 2020 Minnesota protests
- 2020 Puerto Rico earthquake
- 2019 California wildfires
- 2019 California earthquake
- 2019 Hurricanes Barry, Erick
- 2019 Mass shootings – Dayton, El Paso
- 2018 California wildfires

OVERVIEW

A Business Continuity Plan **(BCP)** is used to document information about critical functions performed by key Provider personnel in support of its services performed for Client. The plan is designed primarily as a contingency for disruptions arising from perils directly impacting Providers onsite operations, including the unlikely prolonged disruption of client technology. The plan is also designed to integrate with the Client established business continuity, disaster response, and emergency protocols. In all instances, the goal is to minimize the downtime and financial impact, to all stakeholders, of disruptions resulting from both physical and IT impairments.

The Plan should be reviewed annually and any updates to the process and/or contacts should be made.

PRIMARY ROLES AND RESPONSIBILITIES

Below is an example of how roles and responsibilities might be defined within the plan. It is extremely helpful to spend the time and define these and all info contained within this plan prior to launching the program. Note job titles and responsibilities, expectations and protocols will differ based on the individual Provider and how they define roles and responsibilities, as well as the specific function that is being outsourced and its overall scope.

Leader(s)	
Supplier Operations/Supplier Leads *(serving as the Business Continuity Lead)*	Serve as the Provider's primary point of contact in the event of an emergency. Coordinate necessary staff, and resources, and deploy communications that are consistent with the Provider's scope of services. Provide initial reports and subsequent briefings to Client for matters directly impairing Providers ability to service/manage the program.
Client Key Personnel (Program Sponsors)	Notify Provider Program team of any emergencies that will impact the availability of your facility or any of the resources that are customarily available for Provider to perform its services onsite. Provide initial reports, subsequent briefings, and access to approved mass communications for matters directly impacting Provider operations.
Technology	Ensure the sustainability of the technology platform in a manner which is consistent with your stated recovery objectives. Provide initial reports and subsequent briefings to Client and Provider for matters directly impacting Technology' operations.

BUSINESS CONTINUITY PLAN CONTENTS

I. Business Impact Analysis	• General Information • Minimum Resource Requirements • Key Processes & Recovery Time Objectives
II. Communications Plan	• Activation, Assessment & Action • Returning to Normal Operations • Emergency Contacts • Emergency Conference Call Information • Alternate Meeting Sites
III. Work Instructions	• Work Instructions and tasks for Key Processes • IT Requirements for Remote Network Access ○ Supplier's Network ○ Client Network
IV. Coordination of Crisis Management Plans	• Coordination of Plans • Supplier Corporate Contacts

I. BUSINESS IMPACT ANALYSIS (BIA)

Minimum Resource Requirements

In the event of an emergency that impairs Providers team’s access to their current workspaces or equipment (whether located at a customer site or a home-based remote location), identify the minimum resources required to continue operations. *** *Be clear whether it’s client or Provider owned equipment.*

NOTE: If the Client owns a vendor relationship being utilized, the Ops leader needs to obtain their BCP for the tool.

Resource	Description		
Critical Staff Members	See attached documents		
Laptops/PCs & Monitors	TBD based on location of emergency		
Printer/Fax	Same as above		
Cell/Telephones	Contact information within this plan and on attached documents in **General Information** section above		
Office Supplies	As needed and TBD based on location of emergency		
Internet/Network Access		Supplier Users	Customer Users
	Can users access tools without being logged into the customer’s secured network (i.e., from a non-company network Internet connection)?	Yes	Yes
	Can users access the customer’s secured network remotely?	Yes	Yes

Other Critical Applications	Technology:
	INSERT CLIENT SUPPLIER POLICIES
	INSERT CLIENT SITES TO CONTACT		

<table>
<tr><th>Resource</th><th colspan="3">Description</th></tr>
<tr><td>Critical Staff Members</td><td colspan="3"><table><tr><th>Name</th><th>Title</th><th>Location</th></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr></table></td></tr>
<tr><td>Laptops/PCs & Monitors</td><td colspan="3"><table><tr><th>Name</th><th>Provider Laptop</th><th>Client Laptop</th></tr><tr><td></td><td>Yes</td><td>Yes</td></tr><tr><td></td><td>Yes</td><td>Yes</td></tr><tr><td></td><td>Yes</td><td>Yes</td></tr></table></td></tr>
<tr><td>Printer/Fax</td><td colspan="3">N/A</td></tr>
<tr><td>Cell/Telephones</td><td colspan="3"><table><tr><th>Phone Roster</th><th></th></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table></td></tr>
<tr><td>Hard copy forms</td><td colspan="3">N/A</td></tr>
<tr><td>Office Supplies</td><td colspan="3">N/A</td></tr>
<tr><td rowspan="3">Internet/Network Access</td><td></td><td>Provider Users</td><td>Client Users</td></tr>
<tr><td>Can users access tools without being logged into the customer’s secured network (i.e., from a non-company network Internet connection)?</td><td>Yes</td><td>No</td></tr>
<tr><td>Can users access the customer’s secured network remotely?</td><td>Yes</td><td>Yes</td></tr>
</table>

Key Processes and Process Recovery Objectives (PRO)

The PRO is the maximum amount of time a business process can be interrupted before the impact becomes **severe and unacceptable**. ***Definition:*** Severe and unacceptable means that Provider or CLIENT might miss an obligation that causes either party to violate the law; triggers a significant negative financial impact; causes a breach of contract/SLA; or impairs the ability to ensure the safety of employees. **Use the number scale (1-4) to indicate the PRO for each process.**

The example below assumes that (contingent) workforce has been outsourced in a VMS or RPO outsourced model and should be adjusted based on scope of outsourced services.

Process	**Description**	**PRO** 1: <24 hour 2: 24-48 hours 3: 48-72 hours 4: 1 week+
Receive new job posting	Hiring managers submit requirements via the Technology System and this is reviewed by their Workforce Management team who direct to the VMS tool for open Contingent staffing needs -- this includes: duration, valid cost object information, job title (standard template), Not-to-Exceed Rate, job description, SPU/Business Unit information, timesheet type.	1
Distribute new job postings	Provider distributes the job postings via VMS to suppliers who are qualified to support the labor category (some are distribution list specific).	1
Receive/review candidate submittals	Suppliers submit qualified candidates via VMS. Provider must be able to identify duplicates and eligibility to return. Provider submits final list of candidates for hiring managers' review.	1
Coordinate skills validation	Once hiring managers review candidates, Provider coordinates interviews based on the availability of all interested parties.	3
Candidate selection/offer	Hiring managers select candidates via VMS, generating a Work Order with all of the agreed upon details (dates, rates, etc.). Work Order is subsequently routed through VMS for approval and offer acceptance.	2
On-Boarding activities	Once candidate accepts offer, the Provider and hiring manager initiate on-boarding activities.	2
Timesheet submittal/approval	Once the contractor begins assignment, s/he registers in the VMS and begins to submit timesheets. Provider follows up on pending, draft and unapproved timesheets.	3
Expense sheet submittal/approval	The contractor submits expense sheets for approved business-related travel via VMS. Sheets are automatically routed to customer and customer pays supplier if there are no issues. Provider assists with resolving discrepancies, disputes, or other issues.	3
Miscellaneous invoice submittal/approval	The Provider may submit miscellaneous invoices and approved charges that are to be paid directly to the supplier; not for contractor reimbursement (spot awards, conversion fees, etc.). Provider assists with resolving discrepancies, disputes, or other issues.	4
Credit/debit memo submittal/approval	Credit/debit memos are required to adjust invoices that have been processed by the customer.	4

Invoicing to customer	Invoicing to customer must reflect approved time and must contain accurate and valid cost object information.	4
Payment to Suppliers	Payment to suppliers is made by customer once the invoice has processed. Provider assists with resolving discrepancies, disputes, or other issues.	4
On-boarding new suppliers	New suppliers are on-boarded at the request of customer or upon the recommendation of Provider. On-boarding activities include collection of necessary paperwork, training the supplier on processes and technologies, and creating a supplier record in the VMS.	4
Hiring manager/supplier training	Provider trains hiring manager/suppliers on the VMS technology and key processes on a regular and ad hoc basis.	4
Order management	The provider is required to maintain the data captured in the VMS technology. This includes order extensions, updates to cost objects, order owner/supervisor updates, etc.	3

II. COMMUNICATIONS PLAN

In the event of an emergency that disrupts the Provider's ability to deliver its program management services in a normal manner, the Operations Manager is responsible for executing the plan elements below.

✓	Task Description
Activation	
	Based on the type of emergency, first account for your team members. Determine if any team members are personally affected by the emergency incident. **Refer to Emergency Contacts lists below.**
	Advise team members to not make any statements to the media on behalf of Provider or the customer.
	Advise Provider Leadership that team is activated and the general status of team members.
	Gather preliminary information from customer about the incident (type of incident, general scope of impact, etc.).
	Determine where your team will meet and at what time, using the pre-set meeting locations if appropriate and notify the customer.
	Based on the scope and stage of the emergency, determine how many team members and exactly who needs to be activated.
	Document the availability of each team member, team members you were unable to contact, and any issues.
	For team members who are unavailable, determine if alternate personnel are available to perform designated roles. Escalate any critical resource shortages to Provider Leadership as appropriate.
	As the team assembles at designated points, inform customer of activation/readiness status.

✓	Task Description
Assessment	
	Gather detailed information from customer (or VMS provider), the scope of emergency, and the potential impact to business operations, who is impacted, and initial estimates of any process or system outages (if available).
	Confirm the availability of the team's minimum resource requirements and address any shortages with customer or Provider leadership, if any.
	Obtain regular updates from customer throughout the assessment phase regarding the status of the situation.
	Obtain regular updates regarding the status of assigned tasks from team members throughout the assessment phase.
	Establish communication with vendors, suppliers, and employees to provide an initial status update. Communications should be developed or, at the very least, approved by customer prior to release to suppliers.
	As needed, develop initial draft message(s) to facilitate rapid approval by customer when appropriate.
	Assess the method for which messages will be distributed (email, text, etc.).
	Adhere to the customer's and Provider's media relations guidelines to ensure clarity about any interactions with the media.
	Provide recommendations to customer about content and timing of communications.
Action Phase	
	Activate remote processes as required. **Refer to Task Instructions.**
Returning to Normal Operations	
	Coordinate with all parties to identify any long-term (> 7 days) implications to normal operations associated with the event (i.e. Time card entry mechanism will be unavailable until further notice)
	For any identified issues, ensure proper workarounds are established and functional.
	As appropriate, communicate to internal and external stakeholders as operations resume to normal capacity.
	Debrief with internal team as well as customer and Provider leadership to identify issues/changes for future plan activations.
	Report any required summary information to customer, including successful completion of all team responsibilities.
	Receive approval for team deactivation, release team members to normal functions.
	Synchronize and enter any manually processed data into the VMS tool.
	POST EVENT: Update/enhance team plan and attachments as appropriate to enhance future emergency responses.

Provider Emergency Contacts

Provider Emergency Contacts should be listed in a Provider Contact log and maintained in a specific location <for example MS Teams> and located within this plan.

Client Emergency Contacts

Name, Title	Location	Email

Technology Emergency Contacts

Name, Title	Location	Email and Phone

Alternate Meeting/Work Site #1

(First consider minimum resource requirements when determining alternate work sites. This section is primarily designed for those Operations Managers that perform services from the customer's facilities.)

Name of Facility	**Address**	**Phone Number**	**Primary Contact**	**Wi-Fi Accessible?**
List facility(ies) here	Home addresses or Local Supplier partner local office, if available	See information in documents within **General Information** section above	See information in documents within **General Information** section above	Yes
Reservation required? No	Maximum length of time available? No limit	Is badge access required? No	Is VPN or other technology required? No	Cost of use? None
Map of Location: Remote				

III. WORK INSTRUCTIONS

What you document is repeatable, therefore outlining work instructions for the processes within your specific program enables others to understand what needs to be done and perform those duties in the event of an emergency or extenuating circumstances. A ***Business Process Map*** (refer to the Resource Checklist to learn more) is ideal as it not only lists details, but provides a visual overview of all processes, people, and technology applicable. Value Stream Mapping takes it a step further and allows for a more thorough review of current processes and enables opportunity to identify efficiencies.

Work Instructions for Key Processes

In this section you attach or describe work instructions used for day-to-day program management. The information inserted below is a sample only and references an MSP outsourced program, you will need to customize this, so it reflects instructions for your specific outsourced program. This sample is given to provide an example of the level of detail that should be included.

Process	Instructions
Receive new job posting	• Log in to VMS platform • Inspect Work Items for any new job postings to edit and request intake call • Perform intake call or receive confirmation that intake call is waived • Route job posting for approvals
Distribute new job postings	• Log in to VMS platform • Inspect Work Items for any approved job postings to distribute • Distribute job posting based on template's default distribution list • Perform special distributions for any specific vendors identified and requested by management
Receive/review candidate submittals	• Log in to VMS platform • Review currently open distributed job postings with currently open positions for job seekers needing review • Download or review online the resumes of submitted job seekers and make shortlisting selections • If there is difficulty in receiving job seekers, plan to schedule a spotlight call with the manager and the distributed suppliers to discuss the need
Coordinate skills validation	• If needed, confer with managers to highlight key skills and qualifications that require validation • Contact suppliers to provide additional validation of represented resume items
Candidate selection/offer	• If needed, coordinate interviews with interviewer(s) based on availability and interview type, communicating interview scheduling to supplier to pass on to worker • Log in to VMS platform and mark selected workers as selected for interview (if appropriate) and/or hired following manager selection • Begin the Work Order record in VMS platform and route for management approval

On-Boarding activities	• CPO team supports by notifying suppliers of outstanding onboarding requests prior to worker activation • CPO team requests Contingent ID creation / reactivation for all work orders in Accepted status or later • Suppliers to notify PMO team of onboarding status 2 business days prior to worker start • PMO team to communicate Day 1 details to supplier to share with the worker
Timesheet submittal/approval	• PMO team does not perform activity for timesheet submittal or approval • CPO team reminds suppliers if there are draft timesheets outstanding or remind managers if there are submitted timesheets pending approval
Expense sheet submittal/approval	• PMO team does not perform activity for expense submittal or approval • CPO team reminds managers if there are submitted expenses pending approval
Misc. invoice submittal/approval	• PMO team does not perform activity for miscellaneous invoice submittal or approval • CPO team notify managers if there are submitted invoices pending approval
Credit/debit memo submittal/approval	• PMO team does not perform activity for CDM submittal or approval, except remind managers if there are submitted CDMs pending approval
Invoicing to customer	• PMO team does not perform activity related to invoicing to customer as this is handled centrally from Finance team based on submitted and approved billable expenses in VMS platform and information included in PeopleSoft
Payment to Suppliers	• PMO team does not perform activity related to payment remittance to suppliers as this is handled centrally from Finance team based on received payments from customer and information included in PeopleSoft
On-Boarding new suppliers	• PMO team hosts a program introduction call with supplier to explain next steps and key program elements • Log into Salesforce • Submit a Supplier Enrollment/Change request for a new enrollment (requires supervisor approval) • Following approval, PMO team hands off main responsibility to Supplier Compliance Administration team to lead supplier portal monitoring, but PMO may be involved to share reminders of outstanding items • Following Supplier portal completion, responsibility shifts to VMS platform team for supplier registration, but PMO may be involved to share reminders of outstanding items • PMO team completes supplier setup by sharing key details via a customer-specific template to system administration and then assigning to distribution lists as needed.
Hiring manager/supplier training	• PMO team provides ad hoc consultations as needed when requested over phone or email, leveraging screen sharing (Skype) where appropriate to drive learning • Training resources are available on hiring manager intranet SharePoint for review • VMS platform contains a reference library which includes training materials for both hiring managers and suppliers
Order management	• No orders outside Job Postings / Project Requests are required with the VMS platform in place.

IT Requirements for Remote Access

Accessing Supplier’s Network

All solutions require that you have an Internet connection, either via a home network, Wi-Fi, AirCard, or dial up. Use the format listed below or something similar and detail the requirements for remote access.

<table>
<tr><th colspan="2">For Access To Your E-Mail — Outlook Web Access (OWA) — From Any PC, Anywhere:</th></tr>
<tr><td><b>From any Internet-connected PC or Mac:</b></td><td></td></tr>
<tr><th colspan="2">Network Connect — For Use With a Supplier Laptop:</th></tr>
<tr><td colspan="2">To establish a connection to the Supplier Network, you need <xxxx> installed on your laptop (if applicable). Once you have <xxxx> installed, follow these steps:
1. Click the <b>&lt;xxxx&gt;</b> icon. This will open the login window.
2. Click <b>Authenticate</b>
<i>For assistance, please contact your regional IT Service Desk.</i></td></tr>
</table>

Accessing Client’s Network

Consider whether Provider’s delivery of outsourcing services requires sign-on to the customer’s IT network, noting that in most cases <Provider> employees maintain a distinct login for systems and technology they own and/or manage as well as a Provider business email addresses. In the event of an emergency that requires Provider employees to access the customer’s IT network remotely in order to sustain business continuity, please describe those procedures below.

IV. COORDINATION OF CRISIS MANAGEMENT PLANS

Provider maintains a host of documented crisis management policies and procedures related to evacuation, significant weather events, workplace violence, pandemic, and foodborne illness. However, to the extent that these or other types of perils directly impact or originate from a customer's site, Provider's plans are designed to subordinate to and coordinate with the customer's own established crisis management protocols. Below is a list of key resource examples that may be referenced for the aforementioned matters.

Supplier Global Security & Investigations

Supplier Global Safety, Health & Environmental

Supplier Global Security Programs (Business Continuity)

Supplier Public Relations

Supplier Risk Management

ANNUAL BCP DRILL

Finally, you should include a brief paragraph with information pertaining to an annual drill or test of the plan, outlining who is responsible for initiating and conducting this drill, as well as the timeframe.

For example, you may say something like,

Each year, the <Global Operations Lead/VP> will conduct a drill of the Business Continuity Plan (BCP). The drill will test the BCP plan to ensure the Operations Team is aware of the actions and steps necessary to continue critical business functions after experiencing a disruption to operations in one or more locations or regions. You will be notified after the drill is complete. Any opportunities and/or changes necessary to the plan will be discussed during a formal review of the actions and information learned during the drill. During this review the team will discuss successes and failures of the drill and best practices to keep in mind should a real-life disruption occur in the future.

Make sure your statement reflects the individual responsible for ensuring this drill takes place and the frequency at which a drill will be conducted. Use a table like the one below to document what changes are made to the initial document and when they occurred.

VERSION	DATE OF CHANGE	DOCUMENT OWNER	APPROVED BY	DATE APPROVED	DESCRIPTION OF CHANGES