Business Continuity/ Disaster Recovery Client Response

Table of Contents

1 Introduction

1.1 Purpose

The purpose of this document is to outline the preparedness for potential threats that may impact Pomeroy's operations services, located through-out the US including Pomeroy's Technology Centers (PTCs) and Delivery Centers (PDCs). This document constitutes a formal Business Continuity Management (BCM) response for Pomeroy Clients.

1.2 Restrictions

Standard non-disclosure agreements apply for all recipients of this plan. And, this document should not be shared further without prior written confirmation from Pomeroy.

Pomeroy does not share internal BIA/RAs, Site BC Plans or BC Test Records with Clients as they often hold sensitive Client and contact information, however this document is designed to provide an overview of the plans and processes in place alongside the current position which can be discussed further for specific Clients where required.

1.3 Scope

The scope outlines the key organizational arrangements in place for the Business Continuity Management System (BCMS), any associated policies and strategies. Fundamentally, plans referenced are focused around the safety of Pomeroy employees, continuance of support service operations for all Clients, Crisis Communications, Business Impact Analysis (BIAs), Risk Assessments and Business Continuity Plans (BCPs) and BC plan validation through exercises and tests. Plans should be revised and tested yearly, or as major changes occur.

1.4 Business Continuity Management Team

Under the Information Management Team, Pomeroy has an established and experienced Business Continuity Management (BCM) and IT Service Continuity Management (ITSCM) Capability. Under Executive Management sponsorship, these personnel are responsible for enforcing BCM and ITSCM framework, policies and procedures accordingly. They are responsible for determining local Pomeroy site BC representatives, aiding and guidance around completion of BCM activities, awareness training and BC testing activities.

The ITSCM element of the team works closely with a number of internal business function groups including (*but not limited to*):

- Security Office

- Pomeroy Technology Solutions Team (IT)
- Facilities
- Partner and Alliances Team
- Centralized Service Delivery & Management Teams
- Purchasing and Supply Chain
- Legal
- HR
- Finance

The teams are actively involved in both internal and external BCM & ITSCM audit exercises as part of Pomeroy's regional compliance programs.

1.5 Business Continuity Management Policy

Pomeroy has an established BC Management Policy since 2003. The principles set in this policy describe Pomeroy's approach to maintain continuity of services, as well as defining the responsibilities for the management of business continuity risk at business and individual levels.

The policy is subject to regular audit inspection under the established regional compliance programs and is distributed to Clients where a non-disclosure agreement is in force.

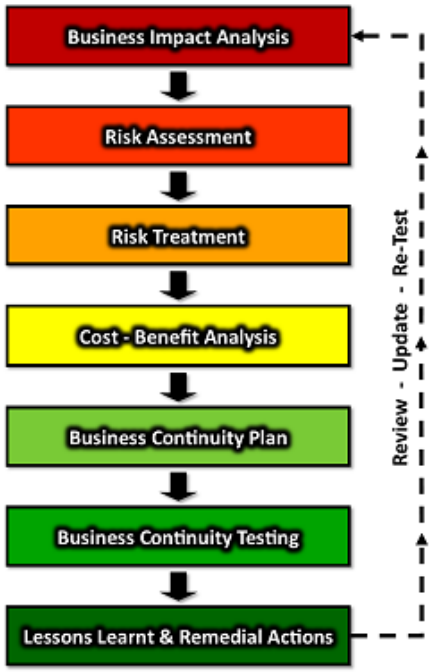
2 Business Continuity Management Overview

2.1 Business Continuity Management System

Pomeroy has an established Business Continuity Management System (BCMS) that follows the ISO 22301 Business Continuity Standard and ISO 27001 Information Security Standard. Pomeroy also adheres to the Business Continuity Institute's (BCI) best practice guidelines in all aspects of its BC Management System.

Pomeroy recognizes the management of BC depends on integration with the organization's strategic and day-to-day management as well as its alignment with business priorities and organizational culture in order to be successful. It is recognized that a sustainable BCM program and the effectiveness of the response to an incident may also depend on challenging and changing culture within the business.

The adjacent diagram highlights the key steps undertaken as part of Pomeroy's BCMS, taking into consideration the Business Continuity Institute's (BCI) best practice guidelines for each level in the *process described.*



2.2 Embedding Business Continuity

The management of BC within Pomeroy depends on integration with the organization's strategic and day-to-day management as well as its alignment with business priorities and organizational culture in order to be successful.

- It is recognized that a sustainable BCM program and the effectiveness of the response to an incident may also depend on challenging and even changing the culture within the business.
- To gain maximum benefit from the BCM program, it is necessary to ensure BC is seen as an integral part of the way things are normally done rather than as a separate activity.
- It is also important to ensure that individuals accept that BC is part of their responsibility and not just something done by BC professionals.

2.2.1 Key Methodology

Developing BC awareness within the company, sustaining a culture of willingness to participate in BC related tasks and achieving belief and support in the BCM program is crucial to its effectiveness. The following are key methods adopted by the organization as a commitment to enforcing this positive BC culture and belief within Pomeroy:

METHODS	METHOD DESCRIPTION
Support & Encouragement from Management	Continued support and leadership by Pomeroy'Management Team should include a budget to support the BCM program. It is also important to gain commitment from Middle Management and operational staff who are required to contribute towards the BCM program.
Consultation	Consultation with those involved in developing the BCM program. As well as providing focus for the awareness effort, consultation helps raise awareness and may help promote commitment to new working practices.
Training, Knowledge, Education & Awareness	Running BC/ITSCM test exercises with employee participation, inclusion of BC awareness in employee induction, involving employees in reviewing and implementing BIAs and BC plans. Setting employee BC objectives.
Addressing Issues & Concerns	Focusing on the business priorities of the organization by addressing any corporate or individual issues and concerns.

2.3 Business Impact Analysis (BIA) Process

Pomeroy recognizes this is a key element of BCM and is the foundation work from which the whole BC process is built and maintained. Undertaking a Business Impact Analysis (and Risk Assessment) for each site location is essential to better understand the organization and its operational needs, and to build/maintain a location BCP that meets the business expectations and requirements.

Pomeroy incorporates the following methodologies as part of its internal BIA process:

- Workshops
- Questionnaires
- Interviews

The BIA data gathering/review process is broken down into two key parts which is meant to identify the severity of impacts to the functions and ability to sustain operations:

Part 1: Business Owners, Customer Representatives and Subject Matter Experts.

This part identifies and reviews the key functions, services and processes. Consideration is given to a number of key aspects including (*but not limited to*):

- Minimum and Optimum staffing levels.
- Maximum Tolerable Period of Disruption (MTPD)
- Recovery Time Objective (RTO)
- Function Inputs, Outputs and Dependencies
- Maximum Tolerable Data Loss (MTDL)

- Recovery Point Objective (RPO)

Part 2: Technology and Applications Managers and Subject Matter Experts.

This part identifies and reviews the key dependent technologies and applications required for Service delivery. This includes Client specific capabilities and internal supporting capabilities. Consideration is given to a number of key aspects including (*but not limited to*):

- Architectural Designs & Resilience Topologies
- Hosting Arrangements
- Technology Dependencies
- Status of DR Plans & DR Testing Capabilities
- Workaround Solutions

2.4 Risk Assessment Process

Pomeroy recognizes that in the context of BCM, a risk assessment looks at the likelihood and impact of a variety of risks that could cause a business interruption and therefore prioritize risk reduction activities.

The process of evaluating threats uses risk assessment techniques to identify unacceptable concentrations of risk to activities and single points of failure, so measures can be considered that may lower the likelihood or decrease the impact of disruption to them.

Used in conjunction with the BIA activities, mitigation measures can be targeted at the most urgent activities within the organization, thus improving the likely return on investment and minimal impact during disruption.

Pomeroy acknowledges and deploys risk management models for BCM.

Key scenarios that are assessed as part of a site Risk Assessment include (*but not limited to*):

- Loss of IT Systems
- Loss of Telecommunications
- Loss of Networks (e.g. MPLS, Internet)
- Loss of Power
- Loss of Utilities (e.g. HVAC, water and/or piped gas supplies)
- Loss of Access to Premises
- Local Transport Issues
- Environmental – Weather
- Environmental – Hygiene and Hazards
- Loss of Staff Services/Facilities
- Loss of Key Staff/Staff Shortages (e.g. Pandemic, Staff Unrest, Political Strike etc.)

- Loss of Key Suppliers
- Cyber Security Incidents
- Site Security Incidents
- Damage to Site
- Total Loss of Site
- Active Shooter/Terrorist Scenario

2.5 Risk Treatment & Cost Benefit Analysis

Standard risk treatment options are considered where required to reduce the potential impacts of identified risks or threats. These include:

- **Avoid:** Where risks cannot be managed to acceptable level, the only option might be to cease or abandon an activity.
- **Mitigate:** Action to minimize the threats and vulnerabilities, to reduce the likelihood of a risk and/or the impact if it occurs. Initiate controls to mitigate potential risks.
- **Transfer**: Share the risk, e.g. by insurance, contractual arrangements, or through partnerships and joint ventures.
- **Accept:** Management accepts the risk on the basis that further mitigation is not cost-effective for the risk's current impact or because any risk reduction strategies outweigh the benefits.

2.6 Business Continuity Plans

Based on the output from the BIA and Risk Assessment process, the construction and maintenance of Pomeroy's BC Plans follows a standard recognized industry approach. The key areas addressed within Pomeroy's BC Plans include:

- Overview of the purpose and scope of the plan.
- Functions, processes, services, client support operations.
- Reference to related documents and recovery plans.
- Key roles and responsibilities.
- Personnel authorized to invoke the BC Plan.
- RACI table.
- Initial actions following an event.
- Commit or Quit assessment.
- Emergency contact telephone numbers.
- Client specific recovery requirements (where applicable).
- Activity Journal used for recording actions and observations during an event.
- Staff notification call process and call tree procedures.
- Major Incident Management scenario descriptions and procedures.

- Business function invocation plans including a 'Default Plan'.
- Site specific details (e.g. reference to site and network schematics schematics).
- Recovery time targets.
- Operational recovery activities including (*but not limited to*):
- Facilities Team
- IT Recovery Team
- HR Team
- Operations Team
- Return to normal activity checklists.

2.7 Business Continuity Testing

Pomeroy recognizes that testing BC Plans is a critical element of the BC Management System. Through testing, Pomeroy can determine the effectiveness of a BC Plan, by exposing issues and further risks as well as being used as a methodology to educate and raise awareness of recovery and response activities for continuity of business operations. It is seen as an activity that helps mature the BC response processes and provides an auditable record for compliance and Client confidence and should not be viewed in a negative manner.

Following Pomeroy's takeover of Pomeroy in the US, the PDCs are undergoing an internal review and update of BIAs, Risk Assessments and BCPs.

These BCPs will be subjected to formal and routine BC Testing procedures accordingly (*minimum annually*) and critical staff performing key functions and / or activities will participate in BC exercises.

Formal test records will be completed as part of this exercise and any issues raised will be followed up accordingly by the BC Management Team.

There are a number of approaches Pomeroy takes to BC testing which range as follows:

- Desktop Exercises - Round table simulations of a BC Plan taking into consideration various scenarios.
- Partial Tests - Rehearsals involving a select group of operational staff.
- Full Tests - Rehearsals involving a whole site or department.
- IT DR Testing - Validating the recoverability of IT infrastructure and Networks.

BC testing strategies may include:

- Manual Workarounds.
- Staff Relocation to Home.
- Staff Relocation to Alternative Premises or Contracted Workspace Environments.

IT DR testing strategies may include:

- Isolated IT DR Testing.
- Live IT DR Testing.

- Network and Telecommunications Switching.
- IT Data Restore Testing.

2.8 Vendor Management & Supply Chains

Pomeroy actively adopts a management program to assess its own third-party and supplier's continuity measures.

This typically includes Data Center colocation partners (PTCs), application delivery partners and critical suppliers of parts.

In the case of PTCs strict hosting, security requirements and standards are enforced, further outlined within this document. For example, Pomeroy ensures that third-party vendors and suppliers have their own R/BCP plans in place.

2.9 Weather Related Events

Pomeroy recognizes the impact that local weather-related events may have on facilities and/or staff's ability to access sites.

Pomeroy uses a number of sites to monitor weather related events. As an example, Hurricanes are monitored through the use of the National Hurricane Center website.

2.10 Active Shooter/Terrorist Threats

Pomeroy recognizes the real threat of an Active Shooter/Terrorist Scenario and has developed an Active Shooter policy. The policy aims to tackle such scenarios where these situations evolve very rapidly and require individuals to make decisions very quickly.

Fundamentally, it is against company policy for employees to bring firearms or dangerous items into a Pomeroy building.

Pomeroy has a clear responsibility to the safety of its staff in such scenarios.

The policy tackles the key procedures and communications to protect staff and maximize survivability using a Security industry best practice of:

- Get Out
- Hide Out
- Keep Out
- Take Out

The policy management system focuses on:

- Prevention/Mitigation

- Preparedness, Education & Training
- Response
- Recovery

While staff are a primary focus as part of such an event, BC Plans would be invoked simultaneously in order to provide continuity of Service operations.

2.11 Cyber Security Threats

Pomeroy implements multiple security policies to safeguard operations. Internal IT systems are actively tested and remediated to minimize the potential for cyber security threats.

Under the Security Division of Pomeroy (*where BCM and ITSCM resides*) there is also an active Security Operations and Governance Team.

2.12 Pandemic Preparedness

Pomeroy has an established Pandemic Preparedness Plan. The plan incorporates the standard phases as follows:

- Interpandemic Phase (Preparedness)
- Alert Phase (Response)
- Pandemic Phase (Response)
- Transition Phase (Recovery)

A Pandemic Response Team is assembled under such a scenario including (*but not limited to*) the following:

- Business Continuity Manager Team Member.
- Health & Safety Representative.
- Human Resources (HR).
- Internal IT Manager.
- Facilities/Real Estate Manager.
- Quality and Security Managers.
- Centralized and Field Based Services Management.
- Procurement and Supply Chain Management.

The BC Manager representative (e.g. CIO or other designated executive) will head the Pandemic Response Team (PRT) and will have a reporting line to the Board during the period of the pandemic.

The members of the PRT will assist with the management of measures to reduce infection, provide subject matter expert advice, and help in making recommendations for Board policy decisions.

Local and global health advice is monitored, reviewed and communicated during such a scenario.

Example communications (internal and external) are included within the plan to;

- Notify employees of precautions and actions that need to be undertaken accordingly.
- Inform Clients of such actions being undertaken and the need to work closely on prevention methods where Pomeroy employees attend Client sites (*e.g. engineers*).

These example communications cover each of the phases outlined.

3 Pomeroy Delivery Centers

The following protections are the standard requirements for all US PDCs. The infrastructure components of the PDCs have been designed with operational criteria that provide continuity protection against outages due to infrastructure failures or force majeure events. The protected areas of the PDCs are categorized as the telecommunications networks, corporate networks, building infrastructure, telephony services, and associate work areas. Pomeroy also employs a series of governing processes across the enterprise, based on the ITIL framework.

Pomeroy's Hebron, KY, campus currently serves as one of the primary Pomeroy Delivery Centers. The campus is nestled on 20 acres within two miles of the Cincinnati International Airport and consists of three buildings.

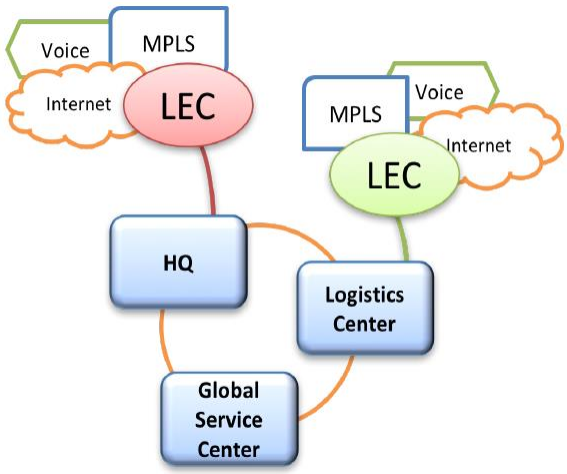
- The Hebron Headquarters building contains the majority of Pomeroy's back-office functions, e.g. finance, IT, executives, etc.
- Two Buildings for the Hebron Logistics Center provides our Logistic Services, National Dispatch Center, Network Operations Center (NOC), Integration Services, and Depot Repair Services.

Pomeroy's Greenville Service Center (GSC) site in South Carolina is located near to Greenville International Airport and serves as the Primary Delivery Center for our Global Service Desk.

3.1 Telecommunication Network

PDCs are serviced by multiple telecommunication carriers and multiple technologies; enabling communication with clients, Pomeroy Technology Centers and other Pomeroy site facilities. Services include local, long distance, and toll-free calling, Internet access, point-to-point data circuits, and MPLS circuits. These services are provisioned and configured to maintain resiliency. Features of the services include:

- The use of multiple carriers for the same service to provide redundancy.
- The use of multiple technologies for the same service for failover capabilities.
- Automated, in-network failover of services between circuits, whenever technically possible.
- Each carrier is required to deliver services into diverse entry locations.
- Each carrier is required to provide services from geographically diverse central offices.



- Carrier circuits are required to have path diversity from their central office (CO) into the PDCs.
- Voice circuits are sized and maintained at 150% of client contracted quantities.
- Internet circuits are sized and managed to 80% utilization.
- Data circuits to PTCs are sized and managed to 80% utilization.

3.2 Corporate Network

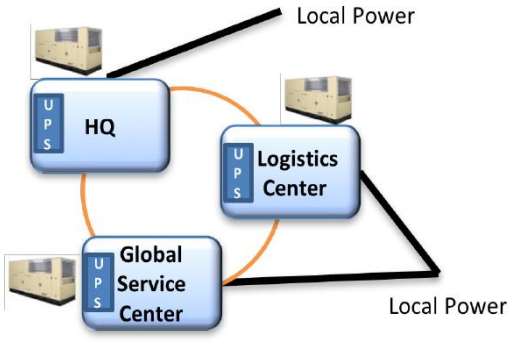
PDCs are designed and built based upon industry best practices, leveraging hardware from industry leading OEMs. Features of Pomeroy's high available network include:

- Layered redundant routing and switching failover capabilities.
- Multiple chassis using dual supervisor engines and protected with dual power supplies, redundant high-speed uplinks, and other high availability best practice configurations.
- Switch capacity designed to N+1.
- Diverse network paths using multiple fiber rings between buildings ensures there is no single point of failure in the PDC Area Network.
- Dynamic routing configured to ensure routes remain available during data network interruptions.
- Redundant Internet circuits from multiple carriers to provide alternate data paths to PTCs or client locations as well as providing connectivity for VPN services.
- Network, Server, Telephony, and Circuit components monitored 24x7x365.
- Network components maintained with 4-hour response SLAs from the manufacturers.

3.3 Building Infrastructure

Each PDC is designed to provide the highest levels of availability. Features of Pomeroy's building infrastructure include:

- Service from the local power grid by two street entrances via diverse substations.
- Each PDC houses one or more power cleansing and protection systems –
- Uninterruptible power systems (UPS) which are sized to operate at 70% utilization at full load.
- UPS power lasts 10-20 minutes. It is designed to maintain equipment functionality until power is restored via the generator.



- UPS devices are configured with fully redundant components and perform twice daily self-diagnostic tests.

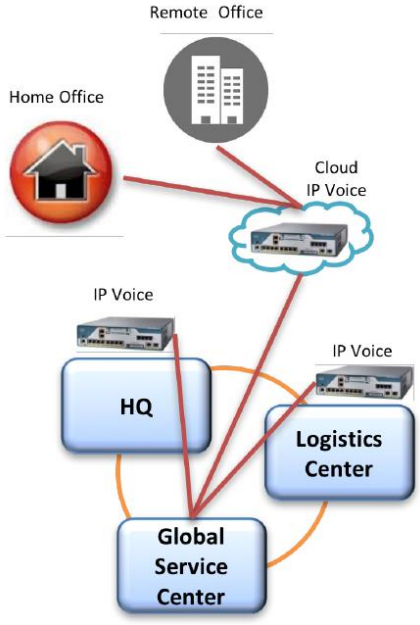
- UPS devices are monitored 7x24x365.
- Each PDC is protected by one or more independent power generation units that are configured to invoke within 10 seconds of loss of street power.
- Power generation units are tested weekly (powered up) and a 24-hour fuel supply is maintained on-site. Additionally, power generator units are tested under full load conditions twice per year.
- Contracts for rapid fuel replacement supplies are in place.
- Lightning protection and proper grounding are designed into each building.
- All PDCs have controlled entrances requiring employees to use a photo badge to gain access.
- MDF and IDF closets are secured to limit physical access to network devices and cabling.
- Security cameras provide real time and historic views of doors and security points.
- Proactive Remote Monitoring of generators to ensure continuous uptime
- A manned security team is on duty 24x7.

3.4 Telephony Services

Pomeroy's Global Service Centers utilize the latest in IP based call center technologies from leading providers. Features of the telephony service and continuity features include:

Two phone switches maintained in separate locations in an active-passive mode.

- Cloud-based telephony system as a means for failover in case of a loss of premise-based telephony service. Voice calls can be redirected within 30 minutes.
- Global Service Center agents can access both the premise based and cloud-based telephony systems from another Pomeroy PDC or a home office.
- Short term continuity protection for inbound calls configured to flow to an in-carrier network voicemail system.
- A cache of cell phones maintained on-site for use in emergency situations that can be issued to agents to access the cloud-based telephone system to provide for short term service continuity.



Pomeroy maintains a contract with a third-party firm for a Cloud based call center telephony service that can be activated upon declaration of a disaster. Client call flows and call scripts are maintained in parallel in both the PDC premised based and Cloud call center telephony services. Upon declaration of a disaster (or extended outage),

Pomeroy's agents may register with the service, providing their primary contact numbers. Pomeroy's inbound toll-free numbers are then re-routed to the service provider. Client calls are processed by the service, follow the standard call flows and call scripts, and then ring to the next available agent registered in the system.

3.5 Associate Work Areas

The associate work areas within the PDCs have been fortified to provide a flexible and robust environment. There are a variety of continuity options available for agents from the handset to the physical work location. Features of the associate work areas include:

- Spare phones, handsets, headsets, computers and monitors on hand for quick support repairs.
- The mobility to work from any workstation and phone within the PDC.
- The capability to work from remote/home offices with access to the same set of service delivery tools.
- Overflow areas available on campus for quick scalability needs of seating agents.
- Workload transfers to other global PDCs (e.g. Service Desk operations where contracts permit).

3.6 Governing Processes

Pomeroy employs a series of governing processes across the enterprise, based on the ITIL framework. Controls have been established for risk assessments, vendor security compliance, and audits of Active Directory, system access, remote access, scan review, and log review. Pomeroy has an established Global IT Security Team & Compliance Team responsible for monitoring the controls that have been established.

4 Pomeroy Technology Centers

4.1 PTC Overview

Pomeroy delivers application and technology services from both Pomeroy Delivery Centers and from Pomeroy Technology Centers (PTCs). For example:

- IT Service Management System.
- IT Asset Management System.
- Field Service and Dispatch Management Systems.
- Knowledge Management System.
- Remote Control Systems.
- Chat Systems.
- Service Depot Asset Tracking Systems.
- Remote Monitoring & Management Systems.
- Integration Service Systems.
- Telephony Services (PDCs and PTCs).
- Network Services (PDCs and PTCs).
- Telecommunications Services (PDCs & PTCs).

Pomeroy currently delivers applications and technology services from Pomeroy Technology Centers via multiple third-party Data Centers located throughout the continental U.S. The Data Center partners used as PTCs have been selected based on a list of criteria including security, reliability, redundancy, and survivability. Each PTC data center partner is required to have a recovery site, corporate backbone and capabilities to meet a 4-hour Recovery Point Objective (RPO) and a 4-hour Recovery Time Objective (RTO). PTC data center providers are required to test their recovery plan at least once per year.

4.2 Partner Data Centers

Pomeroy Data Center partners are required to meet the following criteria:

- Geographic separation between primary and disaster recovery Data Centers of at least 500 miles.
- Primary and disaster recovery Data Centers may not be located in areas that may be susceptible to a single natural disaster or weather event such as an earthquake, flood, tornado, hurricane, etc.
- Be fully hardened facilities that are rated for hurricane, tornado, or seismic risks that may occur in their local geographic region.
- Have multi-layered physical security implemented requiring photo identification, biometric data for entry, and restricted access within the facility to racks and rooms for authorized personnel only.

- Be serviced by multiple telecommunication carriers.
- Have multiple entry points for each telecommunication carriers.
- Require telecommunication carriers to provide service via multiple central offices (COs).
- Configure all network, server and storage equipment with dual power supplies.
- Ensure all network, server and storage equipment receives cleansed and continuous power via an uninterruptible power supply (UPS) and independent power generation systems.
- Provide redundant environmental controls.
- Be capable of operating without street power for up to 96 hours.
- Be rated as a tier II, or higher Data Center.
- Be staffed 7x24x365.
- Located within a 30-mile radius of an airport.

4.3 Applications and Services

Pomeroy's critical applications, whether delivered by Pomeroy or through a SaaS offering, are built to an architectural standard that provides for security, reliability, and high availability. Application infrastructure systems are designed with high availability at each level of the application stack and configured in either an active-active or active-passive mode designed to recover automatically from component or system failures.

Applications and the underlying infrastructure are monitored 24x7x365. Critical applications and data are backed-up, replicated or protected in ways that provide the ability for quick recovery. Critical applications and services provided by third party suppliers are managed through SLAs that meet or exceed Pomeroy's commitments to our clients.

Proof of Conformance – Pomeroy undergoes a SOC2 Type II Audit on an annual basis and requires any partner providing services that support the delivery of applications and technology services to also obtain a SOC2 Type II Audit Report on an annual basis. A copy of Pomeroy's Audit Report is available upon request with an accompanied signed non-disclosure agreement.

5 Crisis Management

Pomeroy has adopted a standard approach to Crisis Management and has developed a framework which is key to managing any crisis event which involves the establishment and practice of essential communications, controls and measurable 'threat-level' classifications.

An overview summary of this framework is described below.

pomeroy™ workplace.optimized.

BCM

Business Continuity Management

Typically used by:

- Emergency Services
- Government Organizations
- Financial Institutions
- Public Transport Companies
- Environement Response Agencies
- Enterprize Business Operations

Crisis Management is often referred to as a hierarchy of control and often takes the form of a Gold, Silver, and Bronze Command Level Structure.

Gold (Strategic)	**Gold Command Team** • Overall Control. Has accountability of organization's finances and resources handling incident. • Authority to articulate strategy for dealing with incident (e.g. prioritize clients) • Responsible for analyzing crisis management progress and managing public relations, insurance, financial decisions, clients, and/or suppliers at highest level.	
Silver (Tactical)	**Silver Command Team** • Assumes tactical command & manages implementation following the strategic direction given by Gold and makes it into sets of actions completed by Bronze. • Assess available resources – deploy these effectively across Scenario Instances • Reports back progress to Gold Command for strategic evaluation • Maintains client contact and facilitates updates (where appropriate)	

Bronze (Operational)	**Bronze Command Team** • Directly controls an organization's resources in managing an incident. • Pro-actively liaises with staff teams on managing task execution. • Co-ordinates recovery or mitigation activities. • Takes tactical direction from Silver Command. • Reports back progress to Silver Command for regular tactical evaluation.	

5.1 Crisis Management Classifications

Pomeroy adopts a recognized scale for determining the classification of any Crisis threat or event. The table below highlights the key 'Alarm Management' classifications, criteria, descriptions and Crisis Management Leading roles:

CLASSIFICATION	CRITERIA & DESCRIPTION	LEADING ROLE
CRITICAL	**Crisis Scenario** ***Board Level Involvement*** A crisis scenario that has had a significant, wide-scale and/or unpredictable impact on Pomeroy's organization and/or Client Service delivery mechanisms/operations. A major impact on site facilities and/or employee safety. Sustained and critical financial impact for Pomeroy and its Clients. Very high claims threaten the continuity of Pomeroy. Sustained and critical damage to corporate image and reputation in market for Pomeroy and its Clients. Requires drastic and urgent actions to be undertaken to overcome the issues. Full-scale Disaster Recovery operation invoked and possible impact on Civil support (e.g. emergency services, government etc.).	**PLATINUM COMMAND** CEO & Board-Level Crisis Management
SEVERE	**Contingency/Calamity Scenario** ***Board Level Involvement*** A crisis scenario that has a significant impact on either internal or strategic Client Service delivery mechanisms/operations. Heavy financial impact for Pomeroy and its Clients. High claims to be expected. Heavy damage to corporate image and reputation in market for Pomeroy and its Clients. Requires very urgent actions to be undertaken to overcome the	**GOLD COMMAND** Corporate Crisis Management

CLASSIFICATION	CRITERIA & DESCRIPTION	LEADING ROLE
	issues. Disaster Recovery operation invoked (part or full). Crucial or strategic Services unavailable.	
SUBSTANTIAL	**Management Escalation Scenario** ***Senior Management Involvement*** A crisis scenario that has a substantial or high impact on either internal or Client Service delivery mechanisms/ operations. Possible financial impact for Pomeroy and its Clients. Claims to be expected. Possible/evidential damage to corporate image and reputation in market for Pomeroy and its Clients. Requires urgent actions to be undertaken to overcome the issues. Infrastructure disruption and some Disaster Recovery operations maybe invoked. Some staff may need to be relocated.	**GOLD COMMAND** Senior Management
MODERATE	**Operational Escalation Scenario** ***Operational Management Involvement*** A moderate level of impact or consequence to either internal or Client delivery mechanisms/operations. Potential/limited financial impact for Pomeroy and its Clients. Claims or fines are possible (Service guarantee failures). Limited damage to corporate image and reputation in market for Pomeroy and its Clients. Requires urgent mitigation actions to rectify/avoid potential or worsening impact. Limited infrastructure disruption is possible, and some recovery operations maybe required. Additional staff maybe required to overcome issues.	**SILVER COMMAND** Operations/Client Management
LOW	**Operational Preparedness Scenario** ***Operational Management Involvement*** A low level of '*potential*' impact to either internal or Client Service delivery mechanisms/operations. Potential risk of financial impact for Pomeroy and its Clients. Risk of claims or fines are possible (Service guarantee failures). Potential risk of damage to corporate image and reputation in market for Pomeroy and its Clients. Requires Crisis Management Preparedness. Requiring some mitigating actions or checks to be carried out. Additional staff maybe required to plan or mitigate potential risks and issues.	**BRONZE COMMAND** Problem Management/MIM
BAU	**Business as Usual Scenario** ***Standard Operational Team Involvement*** Internal Services and functions are running as normal. Standard Operational Services, Teams, and Client Management activities are running as expected. Client SLAs are generally being met. Incidents or issues are being handled via the standard incident management processes with minor to medium disruption. No claims or fines are expected due to service guarantees being met. No current risk of damage to corporate image and/or reputation in market for Pomeroy and its Clients.	**OPERATIONS** Incident Coordinator

5.2 Crisis Communications

Pomeroy has a process for recording crisis threats or events. The event classification will be assessed regularly throughout the lifecycle of such a threat/event. In the event that the likelihood of impact on a US site increases, a Crisis Management Team (CMT) will be deployed following the reporting structure outlined in Pomeroy's Crisis Management Framework.

5.2.1 Potential Threat Communications

Where Pomeroy identifies a potential threat to the site, an entry is registered in the Pomeroy Crisis Management Log. Monitoring of the event continues, and the classification is reviewed on a regular basis. Where the threat increases, Pomeroy may issue communications to its Clients via the Service Delivery Management Teams (Silver Command). The communications will highlight the identified threat and any associated monitoring and/or preparation activities that are being undertaken.

It is recognized that events maybe sudden and unexpected and whilst a Crisis Management log entry will be made and managed, Client communications therefore may commence at the point an invocation is declared.

5.2.2 Invocation - Initial Client Communications

Following a decision to invoke a site BC Plan, communications will be authorized by the Board of Management and sent externally via email in the first instance by the Marketing and Communications Team and/or the VP Security and Compliance (Gold Command).

The initial Client notification will include the following information:

- Confirmation that an invocation has been declared
- Confirmation that a Crisis Management Team (CMT) has been established.
- Outline expectations on recovery timelines.

5.2.3 Invocation - Client Specific Communications

Specifically, Silver Command (Tactical) will be assembled as a team that will not only coordinate resource allocation where appropriate, but also communicate the steps being undertaken with Pomeroy Clients (typically Client Service Delivery Managers).

Clients' own point of contacts will therefore be their relevant Pomeroy Client Service Delivery Manager.

The Recovery Time Objectives for each of Pomeroy's Clients varies and therefore regular communications between Pomeroy and its Clients during an event is handled at a frequency suited to each individual Client via conference bridges and/or direct telephony communications.

Typically, updates will be shared with each Client every 30-60 minutes or as agreed with each Client.

5.3 Crisis Management Toolsets

Whilst Pomeroy has an established methodology for recording, managing and communicating crisis events, the organization has been evaluating the use of numerous Crisis Management toolsets to meet the demands of its growing global operation.

Various industry leading products have been assessed and trials have been conducted. Pomeroy is currently undergoing a cost-benefit analysis for the implementation of such a toolset.

A key advantage of a Crisis Communications toolset is for Pomeroy to be able to communicate more directly and efficiently with Clients around the progress or actions being undertaken during an event where a combination of SMS, Email, Smartphone Push Notifications and rapid emergency conference facilities can be provided.

6 Summary

Pomeroy recognizes the need to ensure confidence with its Clients in its own ability to manage risks, understand threats, continuously review policies, procedures and continuance measures undertaken and ensure all Services and Operations provided to its Clients meets expectations.

This document summarizes at a high-level some of the key measures undertaken and Pomeroy welcomes the opportunity to discuss or answer any specific related questions.