# BRANDON & CLARK

## BUSINESS CONTINUITY PLAN

Critical Infrastructure Support Services - Energy & Municipal Utilities Sector

> **Plan Purpose:** This Business Continuity Plan ensures Brandon & Clark can maintain critical services to oil companies, oil service companies, and municipal power & water utilities during disruptive events, supporting the continuity of critical infrastructure operations.

## 1. EXECUTIVE SUMMARY

### 1.1 Company Profile

| Element | Description |
|---|---|
| **Company Name** | Brandon & Clark |
| **Website** | brandonclark.com |
| **Primary Mission** | Providing professional services to critical infrastructure operators in energy and municipal utilities sectors |
| **Client Base** | • Oil Companies<br>• Oil Service Companies<br>• Municipal Power Companies<br>• Municipal Water Utilities |

| | |
|---|---|
| **Business Criticality** | HIGH - Services support critical infrastructure operations affecting public safety and economic stability |

### 1.2 Plan Activation Authority

| Role | Primary | Alternate | Contact Information |
|---|---|---|---|
| Plan Activation Authority | [CEO/President Name] | [COO/VP Operations Name] | [Phone/Email] |
| Crisis Management Team Leader | [Name] | [Name] | [Phone/Email] |
| Client Communications Lead | [Name] | [Name] | [Phone/Email] |

## 2. CRITICAL BUSINESS FUNCTIONS ANALYSIS

### 2.1 Essential Functions for Critical Infrastructure Support

| Function | Description | Client Impact | Recovery Time Objective (RTO) | Recovery Point Objective (RPO) | Priority Level |
|---|---|---|---|---|---|
| Emergency Response Services | 24/7 emergency engineering/technical support for client incidents | CRITICAL - Potential safety incidents, environmental releases | 2 hours | 0 hours | 1 |
| SCADA/Control System | Industrial control system monitoring | CRITICAL - Loss of | 4 hours | 1 hour | 2 |

| | | | | | |
|---|---|---|---|---|---|
| Support | and maintenance | operational control, safety systems | | | |
| Regulatory Compliance Services | Environmental, safety, and operational compliance support | HIGH - Regulatory violations, fines, operational shutdown | 24 hours | 8 hours | 3 |
| Engineering Design Services | Critical infrastructure design and modification services | HIGH - Project delays, safety system modifications | 48 hours | 24 hours | 4 |
| Project Management | Ongoing project coordination and management | MEDIUM - Project timeline delays | 72 hours | 24 hours | 5 |

## 2.2 Critical Dependencies

| **Dependency Category** | **Specific Requirement** | **Single Point of Failure?** | **Backup Solution** |
|---|---|---|---|
| Personnel | Licensed Professional Engineers | ☐ Yes ☐ No | [Backup PE availability/mutual aid agreements] |
| Technology | Engineering software licenses | ☐ Yes ☐ No | [Cloud-based alternatives/mobile licenses] |
| Communications | 24/7 client communication capability | ☐ Yes ☐ No | [Redundant phone/internet/satellite communication] |

| | | | |
|---|---|---|---|
| Data Access | Client system access and historical data | ☐ Yes ☐ No | [Secure remote access/local backups] |

# 3. CONTINUITY STRATEGIES

## 3.1 Alternate Site Operations

| Site Type | Location | Capabilities | Activation Time | Capacity | Duration Limit |
|---|---|---|---|---|---|
| Primary Office | [Primary Address] | Full operational capability | N/A | 100% staff | N/A |
| Alternate Office Site | [Alternate Address/TBD] | Essential operations only | 4-8 hours | 50% staff | 30 days |
| Home-Based Operations | Distributed/Employee Homes | Remote work capabilities | 2-4 hours | 80% staff | Indefinite |
| Mobile Command Center | Deployable to client sites | Emergency response only | 1-2 hours | 5-10 personnel | 72 hours |

## 3.2 Technology Continuity Solutions

- ☐ Cloud-based engineering software deployment
- ☐ Redundant internet connectivity (primary ISP + cellular backup)
- ☐ VPN access for all critical personnel
- ☐ Laptop/mobile device provisioning for key staff
- ☐ Secure client system access from alternate locations
- ☐ Real-time data synchronization and backup systems
- ☐ Emergency communication systems (satellite phones, radio)

# 4. CRISIS MANAGEMENT ORGANIZATION

## 4.1 Crisis Management Team Structure

| Role | Primary Responsibility | Primary Person | Alternate Person | Key Qualifications |
|---|---|---|---|---|
| Crisis Manager | Overall incident command and decision making | [Name] | [Name] | Senior management, decision authority |
| Operations Coordinator | Service delivery continuity and resource allocation | [Name] | [Name] | Operations management experience |
| Client Relations Manager | Client communication and expectation management | [Name] | [Name] | Client relationship management |
| Technical Services Lead | Technical capability assessment and deployment | [Name] | [Name] | Licensed PE, technical expertise |
| IT/Communications Lead | Technology systems and communications | [Name] | [Name] | IT systems management |

# 5. ACTIVATION PROCEDURES

## 5.1 Plan Activation Triggers

| Trigger Event | Activation Level | Immediate Actions | Notification Requirements |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Natural Disaster (Hurricane, Earthquake) | CRITICAL | • Immediate personnel safety check<br>• Activate alternate site<br>• Client emergency notification | All clients within 2 hours |
| Cyber Attack/IT System Failure | CRITICAL | • Isolate affected systems<br>• Activate manual procedures<br>• Notify clients of potential data exposure | Affected clients within 1 hour |
| Key Personnel Unavailability | HIGH | • Activate succession plan<br>• Reassign critical responsibilities<br>• Client notification if service impacted | Affected clients within 4 hours |
| Supply Chain Disruption | MEDIUM | • Activate alternate suppliers<br>• Assess project timeline impacts<br>• Develop workaround solutions | Affected clients within 24 hours |

### 5.2 Client Notification Procedures

> **Critical Infrastructure Priority:** Given Brandon & Clark's role in supporting critical infrastructure, client notification follows emergency protocols recognizing the potential cascade effects of service disruptions.

| Client Category | Notification Priority | Contact Method | Information Required | Follow-up Schedule |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| Emergency Response Clients | IMMEDIATE (within 1 hour) | • Direct phone call<br>• Emergency hotline<br>• Text/SMS backup | • Service availability status<br>• Estimated restoration time<br>• Alternate contact procedures | Every 2 hours until resolved |
| SCADA/Control System Clients | HIGH (within 2 hours) | • Direct phone call<br>• Email notification<br>• Client portal update | • Impact assessment<br>• Mitigation measures<br>• Recovery timeline | Every 4 hours until resolved |
| Regulatory Compliance Clients | STANDARD (within 4 hours) | • Email notification<br>• Phone follow-up<br>• Written confirmation | • Service impact scope<br>• Compliance deadline impacts<br>• Alternative arrangements | Daily until resolved |
| Project-Based Clients | ROUTINE (within 24 hours) | • Email notification<br>• Project manager call<br>• Client portal update | • Project timeline impacts<br>• Resource reallocation<br>• Recovery expectations | Weekly until resolved |

# 6. RECOVERY PROCEDURES

## 6.1 Recovery Phase Timeline

| Recovery Phase | Timeframe | Objectives | Key Activities | Success Criteria |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| Immediate Response | 0-4 hours | Life safety, damage assessment, emergency services | • Personnel accountability<br>• Emergency client services<br>• Damage assessment<br>• Crisis team activation | All personnel accounted for, emergency services active |
| Short-term Recovery | 4-72 hours | Critical service restoration, alternate site operations | • Alternate site activation<br>• Critical system recovery<br>• Client service restoration<br>• Resource procurement | Essential services operational at 50% capacity |
| Intermediate Recovery | 3-30 days | Full service restoration, temporary normal operations | • Full system restoration<br>• Staff reassignment/augmentation<br>• Vendor coordination<br>• Service level restoration | Normal service levels restored to 80% |
| Long-term Recovery | 30+ days | Return to normal operations, improvement implementation | • Primary site restoration<br>• Lessons learned integration<br>• Process improvements<br>• Plan updates | 100% operational capability restored |

### 6.2 Critical System Recovery Priorities

| System/Service | Recovery Priority | Recovery Time Target | Recovery Steps | Testing Requirements |
|---|---|---|---|---|
| Emergency Communication Systems | 1 | 1 hour | 1. Activate backup communication center<br>2. Test all emergency contact | Full communication with all emergency clients |

| | | | | |
|---|---|---|---|---|
| | | | methods<br>3. Establish client hotline<br>4. Verify 24/7 staffing | |
| Remote Access/VPN Systems | 2 | 2 hours | 1. Verify VPN server functionality<br>2. Test remote access for key personnel<br>3. Validate client system connectivity<br>4. Confirm security protocols | 80% of key personnel can access systems remotely |
| Engineering Software Systems | 3 | 4 hours | 1. Restore software licenses<br>2. Verify data integrity<br>3. Test critical calculations<br>4. Validate client project access | Essential engineering functions operational |
| SCADA/Client Control Systems | 4 | 6 hours | 1. Establish secure connections<br>2. Verify system monitoring<br>3. Test alarm/notification systems<br>4. Validate control capabilities | Critical client systems monitored and controllable |

## 7. RESOURCE REQUIREMENTS

### 7.1 Personnel Resource Planning

| Function | Normal Staffing | Minimum Emergency Staffing | Cross-Training Requirements | External Support Options |
|---|---|---|---|---|
| Emergency Response | [X] personnel | [Y] personnel (24/7 coverage) | All staff trained in emergency procedures | Mutual aid agreements with peer companies |
| Licensed Engineering | [X] PE licenses | [Y] PE licenses minimum | Multiple PEs per specialty area | Consulting PE agreements |
| SCADA/Controls | [X] technicians | [Y] technicians | Cross-training on all client systems | Vendor support contracts |
| IT Support | [X] IT staff | [Y] IT staff | All systems documented, multiple trained | MSP (Managed Service Provider) backup |

### 7.2 Technology Resource Requirements

- ☐ Mobile engineering workstations (laptops with full software suites)
- ☐ Portable communication equipment (satellite phones, two-way radios)
- ☐ Emergency power generation capability
- ☐ Backup internet connectivity (cellular, satellite)
- ☐ Secure remote access tokens/certificates
- ☐ Client system access credentials and documentation
- ☐ Emergency response vehicle(s) equipped with mobile office capability

## 8. TRAINING AND TESTING

### 8.1 Training Program

| Training Type | Audience | Frequency | Duration | Content Focus |
|---|---|---|---|---|
| BCP Awareness | All employees | Annual | 2 hours | Plan overview, roles, basic procedures |
| Crisis Management | Management team | Semi-annual | 4 hours | Decision making, communications, resource allocation |
| Emergency Response | Response team members | Quarterly | 8 hours | Technical procedures, client coordination, equipment use |
| Client-Specific Procedures | Account teams | As needed | Varies | Client emergency procedures, contact protocols |

### 8.2 Testing and Exercise Schedule

| Exercise Type | Scope | Frequency | Participants | Objectives |
|---|---|---|---|---|
| Desktop Exercise | Scenario discussion | Quarterly | Crisis management team | Decision making, communication flow |
| Functional Exercise | Specific system testing | Semi-annual | Technical teams | System recovery, technical procedures |
| Full-Scale Exercise | Complete plan activation | Annual | All staff | End-to-end plan validation |
| Client Integration Exercise | Joint client exercise | As requested | Account teams + clients | Client coordination, service continuity |

# 9. COMMUNICATION PLAN

## 9.1 Internal Communications

| Audience | Information Needs | Communication Method | Frequency | Responsible Party |
|---|---|---|---|---|
| All Employees | Incident status, safety information, work arrangements | Mass notification system, email, phone tree | Initial + every 4 hours | Crisis Manager |
| Crisis Management Team | Detailed status, resource needs, decisions required | Conference calls, secure messaging | Every 2 hours | Crisis Manager |
| Board/Ownership | Strategic impact, major decisions, financial exposure | Direct calls, written updates | Initial + daily | CEO/President |

## 9.2 External Communications

| Stakeholder | Message Focus | Communication Method | Timeline |
|---|---|---|---|
| Clients (Critical Infrastructure) | Service continuity, support availability, impact mitigation | Direct calls, formal notifications, client portals | Per client notification procedures above |

| | | | |
|---|---|---|---|
| Regulatory Agencies | Compliance status, reporting capabilities, remediation plans | Formal written notifications, phone follow-up | As required by regulations |
| Insurance Carriers | Incident details, damage assessment, claim documentation | Claims hotlines, written documentation | Within 24 hours |
| Media/Public | General status, public safety, service restoration | Press releases, company website, social media | As appropriate |

# 10. PLAN MAINTENANCE

## 10.1 Review and Update Schedule

| Review Type | Frequency | Responsible Party | Focus Areas |
|---|---|---|---|
| Complete Plan Review | Annual | BCP Coordinator | All sections, lessons learned integration |
| Contact Information Update | Quarterly | Administrative staff | All contact lists, client information |
| Technology Assessment | Semi-annual | IT Manager | System capabilities, recovery procedures |
| Client Requirements Review | Annual or upon contract changes | Account Managers | Client-specific requirements, SLAs |

# 11. APPENDICES

## Appendix A: Emergency Contact Lists

### Appendix B: Client-Specific Continuity Procedures

### Appendix C: Technology Recovery Procedures

### Appendix D: Vendor Emergency Contacts and Contracts

### Appendix E: Regulatory Notification Requirements

### Appendix F: Insurance Claims Procedures

---

## DOCUMENT CONTROL

| Element | Details |
|---|---|
| Document Version | 1.0 |
| Effective Date | [Date] |
| Next Review Date | [Date + 1 Year] |
| Plan Owner | [BCP Coordinator Name, Title] |
| Approved By | [CEO/President Name] |
| Distribution | • All Management Team Members<br>• Crisis Management Team<br>• Key Account Managers<br>• IT Manager<br>• HR Manager |

> **Plan Activation Contact Information:**
> Emergency Hotline: [24/7 Emergency Number]
> Crisis Manager: [Direct Phone/Mobile]
> Alternate Crisis Manager: [Direct Phone/Mobile]

Company Main: [Main Office Number]
After-Hours: [After-Hours Service Number]

# QUICK REFERENCE GUIDES

## Crisis Manager Quick Checklist

**IMMEDIATE ACTIONS (First 30 minutes):**

1. ☐ Ensure personnel safety and accountability
2. ☐ Activate crisis management team
3. ☐ Assess impact on critical client services
4. ☐ Initiate emergency client notifications
5. ☐ Document incident details and timeline
6. ☐ Establish command center location
7. ☐ Brief executive leadership

**FIRST HOUR ACTIONS:**

1. ☐ Complete damage assessment
2. ☐ Notify insurance carriers
3. ☐ Activate alternate work sites as needed
4. ☐ Deploy emergency response teams
5. ☐ Establish regular communication schedule
6. ☐ Contact regulatory agencies if required
7. ☐ Implement media communication plan

## Client Emergency Notification Template

**EMERGENCY NOTIFICATION SCRIPT:**

"This is [Name] from Brandon & Clark emergency response. We are experiencing [brief incident description] that may impact our services to your facility.

**Current Status:** [Service availability status]

**Estimated Impact:** [Expected service disruption]
**Estimated Restoration:** [Timeline for normal service]
**Immediate Actions:** [What B&C is doing now]
**Your Action Required:** [Any client actions needed]

Your emergency contact for updates is [Name] at [Phone]. We will provide updates every [frequency] until resolution.

Do you have any immediate questions or concerns regarding your critical systems?"

### Technology Recovery Checklist

**SYSTEM RECOVERY PRIORITY ORDER:**

1. ☐ Emergency communications (phone, internet, email)
2. ☐ VPN and remote access systems
3. ☐ Client system access and monitoring
4. ☐ Engineering software and licensing
5. ☐ Document management and file sharing
6. ☐ Accounting and business management systems
7. ☐ Non-critical business applications

**VALIDATION TESTING:**

- ☐ Test client emergency hotline accessibility
- ☐ Verify all critical personnel can access systems remotely
- ☐ Confirm engineering software functionality
- ☐ Validate client system monitoring and control
- ☐ Test internal communication systems
- ☐ Verify data integrity and backup systems

## SPECIALIZED PROCEDURES FOR ENERGY CLIENTS

### Oil & Gas Industry Considerations

| Scenario | Special Considerations | Priority Actions |
|---|---|---|
| Pipeline Monitoring Disruption | • Federal pipeline safety regulations<br>• Environmental release potential<br>• DOT notification requirements | • Immediate operator notification<br>• Backup monitoring activation<br>• Regulatory compliance verification |
| Refinery Control System Support | • Process safety management<br>• Emergency shutdown systems<br>• EPA RMP program compliance | • Safety system status verification<br>• Emergency response coordination<br>• Environmental monitoring |

## Municipal Utility Considerations

| Scenario | Special Considerations | Priority Actions |
|---|---|---|
| Power Grid Support Disruption | • NERC reliability standards<br>• Public safety impacts<br>• Coordinated response with grid operators | • Grid operator notification<br>• Load management assessment<br>• Emergency generation coordination |
| Water System Monitoring Loss | • Safe Drinking Water Act<br>• Public health protection<br>• State health department coordination | • Water quality monitoring backup<br>• Public notification procedures<br>• Alternative water source planning |

---