<Click to insert Facility name here>

**Business Continuity Plan**

<Click or tap to enter a date>

### Version Control

The Site BC Lead/Representative/Other will update this plan on an annual basis or following any significant change to the organisation or key products.

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date updated** | **Person making the change (name)** | **Summary of changes** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Distribution

To ensure the correct version of the plan is in use where hardcopies are printed out, a list of all plan locations and persons supplied with a hardcopy version of this plan should be listed below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Shared with (name)** | **Storage location** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of Contents**

[1. Purpose and Objective 4](#_Toc64975051)

[2. Assumptions 4](#_Toc64975052)

[3. Immediate Response 5](#_Toc64975053)

[3.a. Immediate Response - Process Flow 5](#_Toc64975054)

[3.b. Immediate Response - Emergency Response Procedure 6](#_Toc64975055)

[3.c. Immediate Response - Invoking Procedure 7](#_Toc64975056)

[3.d. Damage Assessment Team Information 8](#_Toc64975057)

[3.e. Damage Assessment Checklist 9](#_Toc64975058)

[3.f. Executive Management Contact List 10](#_Toc64975059)

[3.g. Internal Emergency Contact List 10](#_Toc64975060)

[3.h. Corporate Support Contact List 10](#_Toc64975061)

[3.i Major Safety Incidents 11](#_Toc64975062)

[3.j. Crisis Communications 11](#_Toc64975063)

[4. Recovery Procedures 11](#_Toc64975064)

[4.a. Identification of Business Risks 11](#_Toc64975065)

[4.b. Recovery Strategies 14](#_Toc64975066)

[4.c Recovery Resources Requirements 16](#_Toc64975067)

[4.e Required Applications 20](#_Toc64975068)

[4.f. Vital Records and Data 21](#_Toc64975069)

[4.g. Crisis Command Room (CCR) 21](#_Toc64975070)

[4.h. Key Customer Contacts 22](#_Toc64975071)

[4.i. Key Suppliers Contact List 22](#_Toc64975072)

[4.j. External Services Contact List 22](#_Toc64975073)

[4.k. Pandemic Plan 24](#_Toc64975074)

[5. Control Plan 25](#_Toc64975075)

[5.a. Deactivating the BCP (Standing Down) 25](#_Toc64975076)

[6. Appendix 26](#_Toc64975077)

[6.b. Information Security (Best Practices) 26](#_Toc64975078)

[6.c. Building and Physical Security (Guidelines) 27](#_Toc64975079)

[6.d. Local IT Application Recovery (Best Practices) 27](#_Toc64975080)

[6.e. Table-Top Test Exercise Procedure 27](#_Toc64975081)

# 1. Purpose and Objective

The purpose of the business continuity plan is to identify the top facility / business operational risks, the appropriate preparedness opportunities, and the recovery procedures to be used in response to an event impacting critical business functions. The objective of the business continuity plan is to help establish & maintain a basic level of operations and the continued supply of goods / services following a disruptive event until normal operations can be fully restored.

For more information on the business continuity planning process, please refer to the following corporate policies (if any : Please insert)



# 2. Assumptions

The following assumptions apply to this business continuity plan.

* Formal IT Disaster Recovery Plans (DRP) are outside the scope of this document. The Recovery Time Objective (RTO) information contained in this document will assist in the identification of necessary IT disaster recovery plans, but the specific disaster recovery plans are outside the scope of this document.
* The business continuity plan will be properly maintained and available (hardcopy and/or electronic copy) to the facility management in the event of a facility disruption.
* Corporate and/or private resources will be available to assist with the business recovery efforts as needed.

# 3. Immediate Response

Immediate response will be predicated on many variables, including incident type, impacts and the nature of the business / facility.

## 3.a. Immediate Response - Process Flow

The diagram below provides an overview of the BCP activation process:



## 3.b. Immediate Response - Emergency Response Procedure

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Task** | **Responsible** | **Refer to** |
| 1. | On discovery of a catastrophic event, the facility security and/or Emergency Response Team (ERT) will notify the appropriate local agencies and first responders using communications lists in the Site Emergency Preparedness manual. | Facility, Safety, or Security Leader | Emergency Action Plan |
| 2. | Employee safety is the first priority of Security and Management; therefore Security and Management will protect site personnel through evacuation or movement to secured locations. | Team Leaders | Emergency Action Plan |
| 3. | Facility Leader or ERT notifies the Site Leadership of the event. If the Site Manager will contact the designated replacement   * The Site Leader or Designee contacts the Global Emergency Hotline (if available) to report the event and communicates any immediate assistance needs.   <Click to insert emergency helpline number etc.>   * The Site Leader or Designee contacts the Business Functional Leader to report the event. * The Site Leader or Designee follows the Major Safety Incident Reporting procedure (see appendix) | Facility Leader /  ERT Leader /  Site Leader | Executive Management Contact List  Major Safety Incident Reporting Procedure  (see appendix) |
| 4. | Facility Leader / Emergency Coordinators work with the local agencies and first responders to ensure all personnel are accounted for, secure the facility, and protect Company assets. | Facility Leader /  ERT Leader |  |
| 5. | Follow Site Emergency Action plans and Site Crisis Communication Plans | Team Leaders | Site Emergency Action Plan |
| 6. | Assemble the Damage Assessment Team to assess the facility for:   * Facility – structure and utilities * Equipment – production and telecom, IT * Work in Progress – Finished and unfinished * Office – equipment and any secured files | Facility Leader /  ERT Leader | Damage Assessment Team/Damage Assessment Checklist |
| 7. | Take digital photos of damaged areas for insurance claim and/or communication purposes. |  |  |
| 8. | The Global Emergency Hotline Operator notifies the Crisis Communications Team of the event and communicates any immediate needs for assistance. | Global Emergency Hotline Operator |  |

## 3.c. Immediate Response - Invoking Procedure

This is the proceed of initiation and first steps of a response to a crisis event

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Task** | **Responsible** | **Refer to** |
| 1. | The facility leader and management team are notified that an event has occurred. The facility leader:   * Contacts leadership (as appropriate) and provides an initial assessment of the facility and operations. * Sets an assembly time for the leadership team to gather, gives location and/or conference call number. * Contacts the Crisis Communications team (as necessary) per the Crisis Communications guideline. * Assembles the Functional team (as necessary).   [Notes of the Business Functional Team meeting are to be taken](file:///C:/Documents%20and%20Settings/ah569/Local%20Settings/ah569/Local%20Settings/bg133/Local%20Settings/mdc_data01$/rmp_tech/current%20plan/Current%20Plan/FBU%20Plan/Disaster%20Meeting%20Notes%20Template.doc) | Facility Leader /  ERT Leader | Executive Management Contact list |
| 2. | The leadership team receives initial Damage Assessment report. | Damage Assessment Team Leader | Damage Assessment Checklist |
| 3. | The facility leader and/or executive management team notifies leadership and calls a Crisis Declaration Meeting   * What are is the threat to the business? * What are the potential impacts of the event? * To what extent is the customer at risk? * What is the extent of the damage or outage? * What are the costs associated with the recovery? | Facility Leader /  Exec. Management | Leadership Contact List |
| 4. | Decision to Escalate:   * Does this situation require assistance beyond the local or functional level? * Does this require relocation of people, processes, or materials? * Does the event put customers at risk?   If NO – Operations treats as Contingency, Local Control  If YES – Declare a crisis and implement the appropriate plans and procedures (BCP/DRP/ Recovery Plan etc) | Facility Leader / Exec. Management |  |
| 5. | Facility and executive leadership makes a “Declaration of Crisis” decision and begins implementing the Recovery Plan | Facility Leader / Exec. Management |  |
| 6. | The corporate resources that may be needed to support the Declaration of Crisis are notified.   * Facilities * Risk Management * Environment * Legal * Insurance * HR * Finance * Communications * IT | Team Members | Corporate Contact List |

## 3.d. Damage Assessment Team Information

The Damage Assessment Team will be some of the first people on the scene of the crisis and are responsible for the initial assessment of the site’s ability to operate. The initial assessment completed by this team will be the basis for management decisions for recovery until a more detailed report can be completed. This should be a cross-functional team with members from facilities, security, safety, manufacturing engineering, IT, HR, etc.

The following personnel are the recommended team members.

|  |  |  |
| --- | --- | --- |
| **Contact Person** | **Department** | **Phone #** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 3.e. Damage Assessment Checklist

This checklist is intended to serve as guideline for the Damage Assessment Team in the initial survey of the crisis scene. It should be amended for specific site needs or regional terminologies.

|  |  |  |  |
| --- | --- | --- | --- |
| **Facility** | **Visible Damage?** | **Functional**  **%** | **Comments** |
| **Structure** |  |  |  |
| Walls |  |  |  |
| Roof and Internal Roof Supports |  |  |  |
| Glass Windows, Entry Doors, etc. |  |  |  |
| Bathrooms / Lockers / Showers |  |  |  |
| **Grounds** |  |  |  |
| Parking Area |  |  |  |
| Fire Hydrants |  |  |  |
| Facility Signage |  |  |  |
| **Electric Service** |  |  |  |
| Main Service Feed |  |  |  |
| Building Circuit Panels |  |  |  |
| Internal Electrical Wiring |  |  |  |
| **Non-Structural** |  |  |  |
| Water & Sewer Service |  |  |  |
| Natural Gas Service |  |  |  |
| Security & Fire Alarm System |  |  |  |
| Heating System |  |  |  |
| Data Center Air Conditioning & Controls |  |  |  |
| **Office** |  |  |  |
| Vital Records Storage (Legal file room) |  |  |  |
| Telecom & Network Equipment |  |  |  |
| Conference Rooms |  |  |  |
| Office Furniture |  |  |  |
| Printers / Fax / Copy Machines |  |  |  |
| **Equipment** |  |  |  |
| Stamping & Bending Presses |  |  |  |
| Welding Stations |  |  |  |
| Forklifts |  |  |  |
| Packaging Stations |  |  |  |
| **Work in Process, Inventory** |  |  |  |
| Finished Goods – What is ready to ship? |  |  |  |
| Raw Materials – What is useable? |  |  |  |
| Work in Process – What is useable? |  |  |  |

## 3.f. Executive Management Contact List

The executive leadership is responsible for “chain of command” crisis and recovery decisions.

|  |  |  |
| --- | --- | --- |
| **Contact Name** | **Position / Title** | **Phone #**  **Cell #** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 3.g. Internal Emergency Contact List

The internal emergency contacts needed for local decision making.

|  |  |  |
| --- | --- | --- |
| **Contact Name** | **Position / Title** | **Phone #**  **Cell #** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 3.h. Corporate Support Contact List

Primary contact personnel within each of the key corporate support groups.

|  |  |  |  |
| --- | --- | --- | --- |
| **Internal Contact** | **Department** | **Position / Title** | **Office #**  **Mobile #** |
|  | Enterprise Risk Management |  |  |
|  | Corporate Communications |  |  |
|  | Corporate Security |  |  |
|  | Real Estate/Facilities |  |  |
|  | Corporate Safety |  |  |
|  | Travel Service |  |  |
|  | Corporate Risk Insurance |  |  |
|  | Environmental |  |  |
|  | Legal |  |  |
|  | HR |  |  |
|  | Finance |  |  |
|  | IT Services |  |  |
|  | IT Disaster Recovery |  |  |

## 3.i Major Safety Incidents

In many locations globally there is a legal duty to report certain serious safety incidents. This will be mirrored or enhanced as a Health & Safety Policy requirement.

Should a Crisis Event involve any impact to human safety, it is important that those in Charge of response and Crisis Management are aware of, and follow the appropriate policy and local legislation requirements.

**<Insert Summary or Links to Policy and Legislative requirements>**

## 3.j. Crisis Communications

**< insert a summary or links to crisis communication guidelines >**

# 4. Recovery Procedures

## 4.a. Identification of Business Risks

Business Risk is the potential exposure to an action or event that would have a negative impact on the business’ ability to support its customers. These risks can be naturally occurring, like a tornado or earthquake; man-made like a fire or loss of a key person; or it can be general business risk like a failure of a supplier or failure of an IT application.

There are a range of available resources that review business risks and look forward to upcoming threats (i.e. Business Continuity Institute Horizonscan report)

Shown below is a list of common potential risks. Each facility manager and/or their staff should review this list for potential revisions specific to their operation. Revisions can be made

**Potential Risks to the Facility, Operations, and/or Employees**



Prioritize the risks based on three criteria: Probability, Impact and Vulnerability.

* Probability – the likelihood of an event occurring
  + High – Frequent occurrence
  + Medium – Occasional occurrence
  + Low – Unlikely to occur
* Impact – if the event occurred the effect of the event on the business process
  + High – Business processes are unable to function
  + Medium – Moderate impact to business processes
  + Low – Minimal impact on business processes
* Vulnerability – effectiveness of controls or mitigation implemented by the site
  + High – Unable to detect and/or no risk avoidance measures implemented
  + Medium – Moderate ability to detect and/or some risk avoidance measures in place
  + Low – Easy to detect and/or full risk avoidance measures in place

The best way to identify and prioritize the facility risks is through a facilitated session with participation from the plant manager and his/her immediate staff along with the appropriate facility and safety leaders. The group should have an open discussion about each of the potential risks, and assign a numerical score for the Probability, Impact, and Likelihood of each potential risk.

*NOTE: The typical scoring method is utilized (High = 9; Medium = 3, Low = 1)*

Determine the Risk Priority Number (RPN) by multiplying together the numerical scores for Probability, Impact, and Vulnerability. After determining the RPN for each of the risks, sort the list according to the RPN to determine the highest scoring potential risks. The group should then select the top risks for the development of preparedness and recovery plans.

*NOTE: The group can identify additional risks (despite the voting results) for development of preparedness and recovery plans that are of particular interest or concern to the facility.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Potential Risk** | **Probability (H/M/L)** | **Impact (H/M/L)** | **Vulnerability (H/M/L)** | **RPN Score** |
| Onsite Physical Security Issues | 9 | 9 | 9 | 729 |
| IT Applications Loss | 3 | 9 | 9 | 243 |
| Network Connection Loss | 3 | 9 | 3 | 81 |
| Network / IT Equipment Failure | 3 | 9 | 3 | 81 |
| Loss of People (Internal) | 1 | 9 | 3 | 27 |
| Loss of sensitive info | 1 | 9 | 3 | 27 |

**Above is an example results from a business impact analysis.**

## 4.b. Recovery Strategies

Recovery strategies are the strategies undertaken to enable the facility to survive a crisis event and return back to operations. The key objective of recovery strategies is to quickly identify and address the risks/impacts, stabilize them and direct the recovery of the facility/business.

A step-by-step Recovery Strategy should be developed for each of the key business risks that were identified in section 4.a. An additional recovery strategy should be developed and included for the Catastrophic Loss of the Facility.

### 4.b.1. Recovery Strategy: Key Risk #1

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Task** | **Responsible** | **Refer to** |
| 1. |  |  |  |
| 2. |  |  |  |
| 3. |  |  |  |

### 4.b.2. Recovery Strategy: Key Risk #2

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Task** | **Responsible** | **Refer to** |
| 1. |  |  |  |
| 2. |  |  |  |
| 3. |  |  |  |

### 4.b.3. Recovery Strategy: Catastrophic Loss of Facility (Default)

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Task** | **Responsible** | **Refer to** |
| 1. |  |  |  |
| 2. |  |  |  |
| 3. |  |  |  |

### 4.b.4. Recovery Strategy: Alternative Format



### 4.b.5. Example Recovery Strategy: Power Outage

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Task** | **Responsible** | **Refer to** |
| 1. | Turn-off and/or disconnect any critical pieces of equipment (as appropriate) to minimize the possibility of power surge damage. | Facilities / HSE Manager |  |
| 2. | Notify the electric utility provider of the facility power outage, and determine the expected duration of the electrical outage. | Facilities / HSE Manager | BCP Contact List |
| 3. | Provide the leadership team with information about the facility status and expected duration of the outage, and make a decision regarding the emergency procurement/installation of power generation equipment. | Plant Manager |  |
| 4. | Notify leadership, key customers, and/or key vendors of the facility status, operational plans, and any needs for assistance. | Plant Manager |  |
| 5. | As appropriate, initiate drop-shipments of emergency orders from other distribution centers and/or manufacturing plants. | Outbound Logistics Manager |  |
| 6. | As appropriate, work with local vendors regarding the availability of a power generator for the facility.   * Determine size requirements & delivery schedule. * Coordinate electrical hook-ups with licensed electrician. * Arrange for additional fuel supplies (as appropriate). | Facilities / HSE Manager | Service Provider Contact List |
| 7. | Determine facility staffing requirements during the power outage. | Functional Leaders |  |
| 8. | Notify employees of the event through established communication channels, and coordinate facility staffing levels.   * Email communications * Employee meetings (onsite) * Emergency call list * Local TV and Radio stations | Human Resources / Functional Leaders | Employee Contact Information |
| 9. | Consider the relocation of key employees to remote locations or other facilities during the power outage. | Plant Manager / Functional Leaders |  |
| 10. | Provide the leadership team, key customers, and key suppliers with periodic status updates. | Plant Manager / Functional Leaders |  |
| 11. | Continue to work with the power company to determine when power will be restored. | Facilities / HSE Manager | Service Provider list |
| 12. | Maintain power generation equipment while its in operation. Assign resources (as necessary) to monitor the generator operation and maintain proper fluid levels (fuel, oil, coolant). | Facilities / HSE Manager |  |
| 13. | Once power is restored, work with the facilities group and/or local high-voltage electrician (as necessary) to switch the facility electrical supply from the power generators to outside power. | Facilities / HSE Manager | Generator Shut-down Procedure |
| 14. | Upon recovery, upload any manual data into the production systems and capture/document any lessons learned. | Plant Manager / Functional Leaders |  |

## 4.c Recovery Resources Requirements

The purpose of this section is to identify the equipment and IT applications necessary to re-establish a basic level of business operations following a business interruption. Additionally, this section captures the number of personnel by department during a normal state of operations, and during the first 48 hours of basic operational recovery.

Below is a typical example of a resource recovery matrix. Please adjust and customize this section to suit your business/facility and your Recovery Time Objectives / customer supply requirements

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Business Function** | **Recovery Resource Requirements** | | | | |
| **Personnel Requirements** | | **Equipment** | **IT Applications** | **Dependencies**  **(Internal & External)** |
| **Normal** | **< 2 days** |
| Facilities / HSE | 3 | 3 | Cell Phone, Facility Power, 2-way Radios, Pump Room, Security System, EPA/OSHA Forklifts | Lotus Notes, Maintain-IT, Concur | Electricians  Fire Department  Bldg Inspectors  Koorsen Security  IDI Management  EPA / OSHA (Start-up) |
| Inbound Receiving | 20 | 4 | (2) Reach Trucks, (1) forklift, (4) scan guns, 2-way radio | Order Management System | Transportation Carriers  Outbound Shipping (Space Constraints)  Material Scheduling (Cookeville/Nashville) |
| Transportation | 2 | 1 | 2-way radio, Access to P:/ Drive, | Lotus Notes, P:/ Drive, | RAM Motor Freight  Transportation Carriers |
| Inventory Management | 5 | 1 | Computer, 2-way radio | Lotus Notes,  Order Management System |  |
| Outbound Shipping | 115 | 70 +  Supervision | Pallet Jacks, Order Pickers, Reach Trucks, Sit-down Forklifts, Clamp Truck, Shrink Wrapper, Shop Computers, Label Printers, Scan Guns, Battery Supply, Battery Changing Station, Wireless Network, 2-way radios, portable phone, Copier/Fax Machine, | Lotus Notes,  Order Management System | RAM Motor Freight,  Transportation Carriers  Maintenance Kit Line  Incoming Receiving Group  Inventory Group (Cycle Counts) |
| HR | 3 | 1 | Time Track Sys. Computer, Time Track Time Clock, ADP Time Clock,  Cell Phone, | Time Management System | HR (Payroll / Benefits)  Staffing Services |
| Production Kitting | 4 | 3 | Forklifts, Printers, Computers | Label Software, Order Mgmnt System | Incoming Receiving |

4.d Contingency Planning

### 4.d.1. Contingent Production Plans

This is a list of the key facility products along with the contingent production plans in the event of a significant facility disruption. Please specify both internal and external contingent production plans (if applicable).

|  |  |  |
| --- | --- | --- |
| **Key Products** | **Contingency Plan (Internal)** | **Contingency Plan (External)** |
| Filter XYZ | 1. Shift to another production line. 2. Shift to another plant. 3. Inventory Allocation (EDC, etc) | 1. Repurchase distributor inventory. 2. Temporarily outsource. |
|  |  |  |
|  |  |  |
|  |  |  |

### 4.d.2. Critical Equipment

This is a list of the critical equipment necessary to support the facility operations. The main objective is to identify the critical equipment, and to understand the current status with respect to preventive maintenance (PM), spare parts, service providers, etc.

Equipment may be considered “critical” due to its potential impact on the business, employee safety, or legal requirements. It’s important to note that not all “important” equipment needs to be identified as being “critical”. The following guidelines can be used to aid the identification of critical facility equipment.

* The equipment is one of a kind and/or it’s used for a significant portion of the facility operations such that its failure is unacceptable from business perspective.

Examples would include:

* + - Fork-lifts in a very heavy carton storage area.
    - Wash tank in a Remanufacturing facility.
    - Wireless hand-held guns in a distribution center.
    - Label printers in the shipping department.
* The equipment is the “last line of defense” against an adverse environmental event, or minimizes the risk to employee safety. Examples would include:
  + - Water sprinklers, pressure relief devices, gas/smoke detectors, etc.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Dept.** | **Critical Equipment** | **PM Plans**  **(Y/N)** | **Spare Parts Onsite (Y/N)** | **Key Service Providers**  **(Name / Phone #)** | **Contingency Plan** |
| Paint | Paint Booth | Yes | Yes  (Spray Gun) | XYZ Paint Supply | A) Spray paint by hand with cans.  B) Use local paint shop to spray parts. |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

### 4.d.3. Employee Relocation Plans

This is a list of the key business processes (by department) along with the appropriate employee relocation plans in the event of a significant facility disruption. For temporary disruptions of two weeks or less, it’s recommended that key employees work from home and/or relocate to other company facilities (if appropriate). For facility disruptions in excess of two weeks, you may need to consider leasing temporary space to accommodate key employees or departments.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Emergency Relocation Plans*** | | | | | |
| **Department** | **Headcount** | **Onsite Only?** | **Work from Home** | **Other Plant** | **Local Temp. Space** |
| Facilities / HSE | 3 | Yes | N/A | N/A | N/A |
| Inbound Receiving | 20 | No | N/A | 1st | 2nd |
| Transportation | 2 | Yes | N/A | N/A | N/A |
| Inventory Management | 5 | No | 2nd | 1st | 3rd |
| Outbound Shipping | 115 | No | N/A | 1st | 2nd |
| HR | 3 | No | 1st | 2nd | 3rd |

* Relocation options for other company facilities include: < identify facilities >
* Relocation options for local temporary space include: < identify local space options >

## 4.e Required Applications

This is a complete list of the IT applications (by department function) that are required to support the facility operations. The main objective is to identify the critical IT applications along with the emergency contact information to help restore the application.

Additionally, if an application is locally supported and/or hosted, you should consider having it centrally hosted in the corporate data center to minimize the risk of extended operational downtime. If an application needs to be hosted locally, then a contingency workaround procedure should be developed and documented for the specific application.



## 4.f. Vital Records and Data

This is a list of vital records and data produced and maintained by the facility.

This may include HR records, Financial information, QA data, or ISO Certified facilities this could be a copy of the Record Retention Master List. Key to this table is the location of the backup copies of the records.

It is important to understand the storage location, as if it is off-site (or cloud) then a physical site impact may nor ‘harm’ your records but could create access issues.

|  |  |  |
| --- | --- | --- |
| **Record Name** | **Primary Location** | **Backup Location** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 4.g. Crisis Command Room (CCR)

The facility management team should establish Crisis Command Room (sometimes referred to as an Emergency Operating Center) in preparation for a crisis event. In the event of an emergency, the management team will relocate to the designated CCR (a.k.a. Command Center) which will serve as a base of operations during the operational recovery period.

The primary and contingent CCR information is shown below.

**Primary Location:**

**Contingent Location:**

**Teleconference #:**

**Password:**

**Host:**

## 4.h. Key Customer Contacts

This is a list of key customers that would need to be informed if a crisis event were to impact the facility’s ability to provide products or services as expected by the customer.

|  |  |  |
| --- | --- | --- |
| **Key Customer** | **Contact Person** | **Phone #**  **Cell #** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 4.i. Key Suppliers Contact List

This is a list of key suppliers/ vendor that would need to be informed if a crisis event were to occur to the facility and impact the facility’s ability to utilize products or services produced by the supplier.

|  |  |  |
| --- | --- | --- |
| **Key Supplier** | **Contact Person** | **Phone #**  **Cell #** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 4.j. External Services Contact List

This is a list for quick reference of service providers or local resources that could be needed in the event of a crisis situation. This list would include: police, fire and healthcare providers, statutary agencies or speciality service providers like high voltage electrical maintenance contractors, environmental (spill) recovery, or utility service provier contacts.

Please ammend /delete to suit your local needs

|  |  |
| --- | --- |
| **Service Provider** | **Phone #**  **Cell #** |
| Fire Department |  |
| City Police / County Sheriff |  |
| State Police |  |
| US Marshall |  |
| FBI |  |
| Emergency Management Agencies  (FEMA, Red Cross, etc) |  |
| Emergency Medical Service |  |
| Poison Center |  |
| Hospital |  |
| Property Insurance |  |
| Temporary Staffing Agency |  |
| Natural Gas Utility |  |
| Electric Utility |  |
| Water Utility |  |
| LP Gas Cylinder Provider |  |
| Transportation Providers |  |
| Local TV Station |  |
| Local Radio Station |  |
| FedEx |  |
| UPS |  |
| Copier / Printer / Fax Repair |  |
| Packaging Materials |  |
| Offsite Tape/Document Storage |  |
| Building Utilities Maintenance |  |
| Fire Extinguisher Maintenance |  |
| Fire Sprinkler System |  |
| Snow Removal/Lawn &Lawn Sprinkler |  |
| Overhead Door Repair |  |
| Forklift Repair |  |
| Water Pump Room |  |
| County Building Inspector |  |
| Environmental Protection Agency |  |
| OSHA Worker Safety Agency |  |
| Electrical Contractor |  |
| Plumbing Contractor |  |
| HVAC Contractor |  |
| Building Signage |  |
| IT Cabling |  |
| Security Gates & Fencing Contractor |  |
| Waste & Recycling Services |  |
| Cleaning Service |  |

## 4.k. Pandemic Plan

The facility management team should familiarize themselves with the Company’s Pandemic Plan and determine the appropriate level of pandemic preparedness for their facility.

|  |  |  |
| --- | --- | --- |
| **#** | **Pandemic Preparedness** | **Responsible** |
| 1. | Familiarity with company’s Pandemic Protection Policy. | Plant Manager / Safety Leader |
| 2. | Familiarity with World Health Organization pandemic guidelines. | Safety Leader |
| 3. | Install and encourage use of alcohol-based hand sanitizer within the facility. | Safety Leader |
| 4. | Print & Distribute any available preparedness posters throughout the facility. | Safety Leader |
| 5. | Identify a facility isolation room to be used in the event of a breakout.  NOTE: The isolation room should be at the end of a corridor and feature a door that can be kept closed. Any preventative equipment should be stored in the room. | Plant Manager / Safety Leader |
| 6. | Purchase a minimum quantity of protective equipment (gloves, masks, etc) for onsite storage in the event of a break-out. | Safety Leader |
| **#** | **Pandemic Recovery Procedure** |  |
|  | *NOTE: The Pandemic recovery procedure should be taken directly from the company’s Pandemic Protection Plan.* |  |
|  |  |  |

# 5. Control Plan

This section addresses the control processes that will be used to ensure that the business continuity plan is properly maintained. **TBD** has been identified as the local BCP leader for the facility, and he/she will be responsible for the control plan items.

The local BCP owner will also be responsible for the distribution of the plan to site management and key employees. It is highly recommended that key site personnel keep a hardcopy of the plan in an offsite location (personal residence, automobile, etc) that is convenient to them. Additional hardcopies should be maintained onsite perhaps in tabbed binders along with the other key facility plans. Soft copies of the continuity plan could be stored on personal computers, network drives or removable media.

| **BCP Component** | **MIN Update Frequency** |
| --- | --- |
| Purpose & Objective | **Annual** |
| Document Distribution | **Annual** |
| Recovery Procedures | **Annual** |
| Table-Top Test Exercise  (Appendix section 6.e) | **Annual** |
| Contingency Plans | **Annual** |
| Contact Lists | **Annual** |
| Key Equipment | **Annual** |
| Required Applications | **Annual** |
| Vital Records | **Annual** |
| Pandemic Plans | **Annual** |

***\* May require more frequent updates due to employee turnover, vendor changes, etc.***

**NOTE:** The business continuity plan should be revisited in the event of a facility move and/or significant operational changes. In such a case, the local BCP leader shall convene a session with facility leaders to revisit and update the complete continuity plan (operational risks, preparedness needs, recovery plans, etc.)

## 5.a. Deactivating the BCP (Standing Down)

The following roles have the authority to deactivate the Business Continuity Plan and stand down the recovery process:

* Insert Site Director/Other
* Insert Site Crisis Management Team Lead/Other
* Insert Site Business Continuity Lead/Other

# 6. Appendix

### 6.a.1. Preparedness Opportunities

A list of preparedness opportunities for each of the key business risks (refer to section 4.a).

### 6.a.2. General Preparedness (Example)

* Ensure key employees have laptop computers to enable remote access.
* Ensure key employees have mobile phones.
* Purchase a satellite phone for the facility to aid emergency communications.
* Reinforce the information security best practices (**See Appendix 6b**).
* Locked and fire-proof storage for onsite vital records.
* Cross-training and/or Succession planning for key facility roles.
* Maintain spare parts and/or redundancy for key facility equipment.

### 6.a.3. By Risk (Power Outage Example)

* Investigate Power Generation equipment & installation for the facility.
  + Power Generation size requirements, costs, and emergency availability.
  + Facility wiring needs and cost estimates.
  + Identify an emergency fuel source.
* Pre-cable the facility for emergency power generator installation. (MINIMUM)
* Purchase / Install standby power generation equipment.

## 6.b. Information Security (Best Practices)

* When away from your desk, lock your computer screen using (Ctrl + Alt + Delete).
* Sensitive company and/or employee data shouldn’t be loaded onto removable devises.
* Important files should be saved to a network drive in addition to the computer hard drive.
* Employees should take laptop computers home with them (evenings and weekends).
* Confidential conversations should take place only behind closed doors.
* When printing sensitive information, collect the material from the printer immediately.
* Do not keep sensitive information in clear view within your workspace.
* Use a privacy screen when using your laptop in public places.
* Don’t discuss sensitive company matters in public places.
* Utilize secure file transfer when transmitting sensitive data

## 6.c. Building and Physical Security (Guidelines)

* Facility access is limited to entrances/exits deemed necessary by Plant Manager.
* Facility should have a visitor entrance and holding area.
* Entrances/Exits must have reliable method to identify employees & guests.
* Building should utilize fencing or natural barriers to indicate a security presence.
* Buildings should have physical security and/or an appropriate alarm system.
* Lighting of building exterior and parking areas should be provided where applicable.

## 6.d. Local IT Application Recovery (Best Practices)

* Important IT data should be saved (backed-up) every 4-6 hours.
* Back-up media should be stored offsite at least 50 miles away.
* Maintain spares for critical equipment and/or replacement parts.
* Maintain documentation of system components and capabilities.
* Maintain interoperability between primary and any alternate site equipment.
* Server room air temperatures should be maintained between 68F – 72F.
* Server room floor should be raised 6” – 12” to allow for cooling, cable storage, etc.
* Server room should have a system of fire detection and suppression.
* Consider installing an Uninterruptable Power Supply (UPS) system.

## 6.e. Table-Top Test Exercise Procedure

* The local BCP Leader develops a potential crisis scenario based on facility and/or operational risks. The scenario should be practical and structured in a chronological sequence of events.
* The BCP Leader should also develop a list of key considerations and actions associated with each stage of the test scenario, and schedule time with the facility management to discuss the scenario.
* The BCP Leader presents the scenario to the management group in stages, pausing after each stage to allow sufficient time for the management group to identify & discuss the appropriate tasks and responsibilities for the scenario.

*NOTE: The BCP leader should facilitate the discussion as needed and utilize the list of key considerations to spark the conversation when appropriate.*

* Upon completion of the individual stages and/or overall test exercise, the BCP leader should provide feedback to the management group on the quality/completeness of their identified actions relative to the guidelines set forth in their business continuity plan.
* The BCP leader should solicit feedback from the management group on the format and benefits of the exercise, and he/she should initiate conversation on future test scenarios (specific scenarios of interest, testing frequency, key participants, etc).
* The BCP leader should document the completed test exercise, and schedule future test sessions as directed by management group and/or as specified in the BCP control plan.