Aberrant Open-ISM™

BUSINESS CONTINUITY AND DISASTER RECOVERY POLICY

Property	Description
Document Version	1.0
Status	DRAFT
Last Update	2022-03-25
Document Owner	Risk Management

PROPRIETARY

Next Scheduled Review		
Document Approvals		
Approver Name	**Title**	**Date**
???	???	???

Revision History			
Version	**Date**	**Description of Changes**	**Revised by**
1.0	2022-03-25	DRAFT	Aberrant

TABLE OF CONTENTS

1 OVERVIEW

The purpose of the Business Continuity Plan is to provide a single framework for all business continuity and disaster recovery activities. The overarching aims of the program are the following:

- To provide a transparent and maintainable management system for addressing risk.
- To prevent, or reduce, undesirable outcomes.
- To achieve continual improvement.

2 SCOPE

The Business Continuity Plan will provide holistic guidance for the identification and management of risk. The plan is designed to provide specific instructions for implementing operational controls that will allow the organization to monitor, measure, and ultimately address disruptive incidents. Responsibility for maintaining the plan falls squarely within the ambit of information security.

3 LEGAL AND REGULATORY REQUIREMENTS

The organization shall establish, implement and maintain a procedure(s) to identify, have access to, and assess the applicable legal and regulatory requirements to which the organization subscribes related to the continuity of its operations, products and services, as well as the interests of relevant interested parties.

The organization shall ensure that these applicable legal, regulatory and other requirements to which the organization subscribes are taken into account in establishing, implementing and maintaining its Business Continuity Management System (BCMS).

The organization shall document this information and keep it up-to-date on at least an annual basis. New or variations to legal, regulatory and other requirements shall be communicated to affected employees and other interested parties. Copies of the plan will be kept by each member of the management team and other key members of the recovery team.

4 CRISIS RESPONSE TEAM RESPONSIBILITIES

The Crisis Response Team is responsible for establishing, implementing and incrementally improving the plan. The Crisis Response Team, and top level management, shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization by:

1. Defining the criteria for accepting risks and the acceptable levels of risk.
2. Actively engaging in exercising and testing.
3. Ensuring that internal audits of the Business Continuity Plan are conducted.
4. Conducting management reviews of the Business Continuity Plan.
5. Demonstrating commitment to continual improvement.

5 CRISIS TEAM COMPETENCE

To effectively perform Business Continuity responsibilities, Crisis Management Team members should have the requisite industry experience and professional qualifications necessary to perform tasks in a competent manner. Prior to assignment to the Crisis Management Team the organization should:

1. Determine the necessary competence of person(s) doing work under its control that affects its performance.
2. Ensure that the employee in question is competent on the basis of appropriate education, training, and experience.
3. Where applicable, take actions to ensure that team members acquire the necessary competence.
4. Retain appropriate documented information as evidence of competence.

Applicable actions can include, for example: the provision of training to, the mentoring of, or the reassignment of current employed persons; or the hiring or contracting of competent persons.

6 CRISIS RESPONSE TEAM

In the event of an emergency, it is essential that a group of <<Company Name>> employees are trained to respond to disasters and present information in a calm and timely manner to ensure that members and staff are secure and the public and the media are accurately informed. The members of <<Company Name>>'s Crisis Response Team will include:

Role	Primary Responsibility
Primary Crisis Manager / Communication Coordinator	To oversee the entire crisis response team.
Back Up Deputy Crisis Manager	To direct operational, distribution, marketing, and administrative activities prompted by the crisis.
Communication Coordinator	Responsible for all public and media relations during crisis and to coordinate whatever communication and community relations assistance is needed.
Legal Coordinator	To provide whatever legal assistance may be needed at the site in crisis or within the business.
Administrative Coordinator	Responsible for 24-hour phone coverage and to communicate with the general membership regarding the crisis.

7 CRISIS RESPONSE TEAM EMERGENCY CONTACT INFORMATION

The appropriate Crisis Response Team members need to be notified when an emergency has been identified. The following contact information has been distributed to employees and they are instructed to reach out to the Crisis Response Team to provide notification of a disaster. Crisis Response Team leaders will also be monitoring for natural disasters such as winter storms, hurricanes or possible flood weather.

Role	Designated employee	Phone	Email
Primary Crisis Manager / Communication Coordinator	<<Name and Title>>	<<Phone Number>>	<<Email>>
Back Up Deputy Crisis Manager	<<Name and Title>>	<<Phone Number>>	<<Email>>
Communication Coordinator	<<Name and Title>>	<<Phone Number>>	<<Email>>
Legal Coordinator	<<Name and Title>>	<<Phone Number>>	<<Email>>
Administrative Coordinator	<<Name and Title>>	<<Phone Number>>	<<Email>>
IT Crisis Coordinator	<<Name and Title>>	<<Phone Number>>	<<Email>>

8 EMPLOYEE AND CONTRACTOR RESPONSIBILITIES

Persons doing work under the organization’s control shall be aware of:

1. The business continuity policy.
2. Their contribution to the effectiveness of the Business Continuity Plan, including the benefits of improved business continuity management performance.
3. The implications of not conforming with the requirements of the Business Continuity Plan.
4. Their own role during disruptive incidents.
5. Employees or contractors who detect or suspect an information security event has occurred should immediately notify support personnel.
6. All employees or contractors should note and immediately report any observed or suspected security weaknesses in any information processing system or service—security vulnerabilities must be reported first before a fix is attempted.

9 DESIGN METHODOLOGY

The organization has developed and implemented a comprehensive Business Continuity Plan, which encompasses the following categories and supporting activities listed below. These policy directives will be fully enforced, and monitored, to ensure that Business Continuity Plan initiatives are executed in a timely manner and on a consistent basis for all system components within the data environment and all other I.T. resources deemed critical by the organization. The seven (7) main categories of the plan include the following:

1. Risk Assessment: The organization needs to assess potential risks to the business: e.g. critical business functions, infrastructure, and personnel.
2. Resilient Design: Critical business functions and supporting infrastructure must be designed in such a way that it incorporates redundancy and spare capacity to mitigate against operational error or equipment malfunction.
3. Recovery Procedures: Arrangements must be made to recover, or restore, business functions when either prevention or resilience fail.
4. Contingency Planning: The organization establishes a generalized capability and readiness to cope effectively with whatever major incidents and disasters occur, including those that were not, and perhaps could not have been foreseen. Contingency preparations constitute a last-resort response if resilience and recovery should prove inadequate in practice.
5. System Monitoring: Establish, implement and maintain procedures for detecting, logging and alerting operational personnel of security incidents or system outages.
6. Training, Testing, and Review: Personnel must be periodically trained on proper operational procedures. Systems and operational processes must be empirically tested on an annual basis to ensure that business continuity procedures are an effective remedy for disaster incidents.
7. Continuous Improvement: Feedback captured from testing should be used to update the business continuity and disaster recovery plan.

Please note that all requirements for regulations for the plan are included in the seven (7) previously listed categories, which have been identified as a best of breed framework for developing and implementing an effective Business Continuity Plan.

10 RISK ASSESSMENT

The Enterprise Risk Policy provides details on how the organization evaluates risk. The Enterprise Risk Policy must account for business continuity and disaster recovery since it is the foundation for the organizations preparation for contingency planning.

11 RESILIENT DESIGN

11.1 REMOTE WORK AND ESSENTIAL STAFF

Essential staff are issued laptops and have access to VPN so that they can work remotely from any location. The configuration and use of laptops must conform to <<Company Name>>'s Acceptable Use Policy.

11.2 CLOUD BASED INFRASTRUCTURE

<<Company Name>> maintains servers and systems remotely. As a result, access or damage to facilities has minimal impact on the company's ability to provide service to our customers.

11.3 RESILIENT DESIGN AND HIGH AVAILABILITY

When possible system are designed to be stateless to support elastic scale. In the case of stateful systems redundancy is considered a system requirement. Our primary active datacenters have redundant servers, systems and devices to ensure that the failure of any single device does not result in a service outage for our customers.

11.4 FAILOVER ACROSS REGIONS

Redundant system are available across regions in the event of a cataclysm that impacts one specific region.

11.5 DISASTER RECOVERY AS A SERVICE (DRAAS)

When possible we leverage cloud-based DRaaS system in preference to building and supporting our own systems.

11.6 ISOLATION AND COMPARTMENTALIZATION

Networks, systems and data are logically isolated for the purpose of encapsulating risk. When incidents do occur, encapsulation helps to limit the spread of damage which makes disaster recover more manageable.

12 RECOVERY PROCEDURES

Please see the Data Recovery Policy for details on backup recovery.

13 CONTINGENCY PLANNING

13.1 LEVEL 1: INFORMATION SECURITY

Information security is an integral component of the plan. All business continuity planning and activities related to information security should conform to information security requirements.

13.1.1 INFORMATION SECURITY SCENARIOS

13.1.1.1 DATACENTER FAILURE

<<Company Name>> maintains two geographically separated datacenters in an active-active configuration. Our primary datacenter is located at AWS located in North Virginia; Our secondary active datacenter is located at AWS in Oregon.

13.1.1.2 NETWORK INTRUDER

In the event of a network intruder the IT Crisis Coordinator, or IT staff member, would notify the Crisis Response Team that unauthorized access has been detected on the network. The IT Crisis Coordinator would then work with the Incident Response Team to address the issue in accordance with <<Company Name>>'s Incident Response Plan.

13.1.1.3 DATA BREACH

In the event of a data breach, where sensitive customer information has successfully been removed from the <<Company Name>> network, or systems, the Crisis Response Team will be notified when the breach is discovered. The IT Crisis Coordinator will then act in accordance with the Incident Response Plan. The Communication Crisis Team member, working with the Incident Response Team, will reach out to the required authorities, such as the Attorney General, notifying them that a breach has occurred on <<Company Name>>'s systems and sensitive customer information has been taken. The Business Continuity and Disaster Recovery Plan contains templates for communication to customers and the public if data were to be exposed in this fashion. If an internal employee was behind the leak, that employee will face discipline for violating policy.

13.1.1.4 DISTRIBUTED DENIAL OF SERVICE ATTACK (DDOS)

The IT Crisis Coordinator will work with external vendors to ensure that the site stays available to customers. If the IT Crisis Coordinator is unable to prevent a disruption in service, then he/she will notify the Crisis Response Team. The Communication Crisis Team member, working with the Incident Response Team, will communicate externally to customers the status and share mitigation efforts as necessary up to the conclusion of the attack.

13.1.1.5 TECHNICAL DISRUPTIONS / DISASTERS

Network Failures, Data Communication Disruptions, Power Disruption and Voice Communication Disruption can lead to a failure in completing business tasks. In the case of any of these disruptions of service, the utility vendor should be contacted and a determination of restoration of services should be provided. A network failure would need to be checked by the IT Crisis Coordinator before confirming that the ISP or other service provider would need to be contacted. After a power outage, all UPSs should be retested to verify functionality. A list of vendor contact information has been included in this document. If the outage is longer than what is deemed feasible for continuing business, then the Crisis Response Team would need to determine if employees should work remotely.

13.1.1.6 CRITICAL EQUIPMENT FAILURE / HUMAN ERROR

Human error or faulty equipment can result in a system outage. Initially, it may be difficult to ascertain a benign system failure from a security breach. In the event of a system failure the IT Crisis Coordinator will act in accordance with the Incident Response Plan. The Communication Crisis Team member, working with the Incident Response Team, will reach out to customers that have been affected. The Disaster Recovery Plan contains templates for communication to customers.

13.1.2 CRISIS TEAM RESPONSIBILITIES / DUTIES

In addition to the requirements above the members of the Crisis Response Team have the following duties during and after a Level 1 disaster event.

13.1.2.1 PRIMARY CRISIS MANAGER DUTIES

Contact board members, key officials and clients to explain the situation.

13.1.2.2 DEPUTY CRISIS MANAGER DUTIES

Provide Communication Team with frequent on-site updates.

13.1.2.3 COMMUNICATION COORDINATOR DUTIES

1. If appropriate, issue a news release.
2. If needed, prepare spokesperson for media briefing.
3. Address all media concerns.
4. Prepare statements.
5. If needed, coordinate press conference(s).
6. Track all media coverage with the assistance of other Corporate Communication staff and immediately respond to inaccurate information.

7. If there is a data breach, prepare statements to the appropriate authorities and customers. Information should include:
    0. A detailed description of the nature and circumstances of the breach of security or unauthorized acquisition or use of personal information;
    1. The number of Massachusetts residents affected as of the time of notification;
    2. The steps already taken relative to the incident;
    3. Any steps intended to be taken relative to the incident after notification; and
    4. Information regarding whether law enforcement is engaged investigating the incident.

13.1.2.4 LEGAL COORDINATOR DUTIES

1. Call back-up counsel if needed.
2. Document all interaction during the day, including meetings, press conferences, etc.

13.1.2.5 IT CRISIS MANAGER DUTIES

Determine the extent of the damage to the current systems, what data can be recovered and if new equipment needs to be purchased.

13.2 LEVEL 2: REGION DISRUPTION

Level 2 crises relate to issues that might affect remote staff.

13.2.1 REGION DISRUPTION SCENARIOS

13.2.1.1 NATURAL DISASTERS AND RIOTS

A regional disruption such as a natural disaster or a social disruption like a riot could result in home evacuations or internet service disruptions for staff working from home. A disruption of this type could potentially reduce the number of staff that are able to perform work remotely. To address this issue staff have been cross-trained and instructed on shared duties to complete normal job tasks to account for this scenario. <<Company Name>> also makes every effort to hire for redundancy to ensure that succession from turn-over or promotion doesn't result in a work stoppage.

13.2.2 CRISIS TEAM RESPONSIBILITIES / DUTIES

In addition to the requirements above the members of the Crisis Response Team have the following duties during and after a Level 1 disaster event.

13.2.2.1 PRIMARY CRISIS MANAGER DUTIES

1. Contact all department managers to request that their staff be called and informed to take appropriate action, e.g. evacuate, shelter in-place, etc.
2. Contact board members, key officials and clients to explain the situation.
3. If there are casualties, contact the family of the victims within 24 hours to express sympathy and support.

13.2.2.2 DEPUTY CRISIS MANAGER DUTIES

1. Provide Communication Team with frequent updates.
2. Address any public concerns with approved briefing information.
3. Provide on-site media and family with approved information and contacts.

13.2.2.3 COMMUNICATION COORDINATOR DUTIES

1. If needed, issue a news release.
2. If needed, prepare spokesperson for media briefing.
3. Address all media concerns.
4. Prepare statements.
5. If needed, coordinate press conference(s). Track all media coverage with the assistance of other Corporate Communication staff and immediately respond to inaccurate information.

13.2.2.4 LEGAL COORDINATOR DUTIES

1. If casualties, call the victims' emergency contacts.
2. Answer any questions or concerns from staff or family members.
3. Call back-up counsel if needed.
4. Document all interaction during the day, including meetings, press conferences, etc.

13.2.2.5 ADMINISTRATIVE COORDINATOR DUTIES

1. If accessible, leave a voice message on the main telephone system.
2. Get phone lines in order. If needed, contact staff to assist in answering phones or helping with other administrative duties (crowd control, tours, etc.).

13.2.2.6 IT CRISIS MANAGER DUTIES

Determine the extent of the damage and if new equipment needs to be purchased.

13.3 LEVEL 3: LOSS OF PERSONNEL

Level 3 crises pertains to the sudden loss of personnel.

13.3.1 PANDEMIC

The main goal in Pandemic Response is to protect the employees' health and safety in addition to limiting the negative impact to the organization. A pandemic incident could lead to the following scenarios:

- Higher than normal rates of absenteeism
- Government induced travel restrictions or full or partial quarantines
- Public health mandated isolation policies
- Disruption of power, communications or other essential services

The guideline on Pandemic Response and preparation will look to address:

1. Establishing an ethic of infection control in the workplace that is reinforced during the annual influenza season, to include, if possible, options for working offsite while ill, systems to reduce infection transmission and worker education;
2. Establishing contingency systems to maintain delivery of essential goods and services during times of significant and sustained worker absenteeism;
3. Where possible, establishing mechanisms to allow workers to provide services from home if public health officials advise against non-essential travel outside the home; and
4. Establishing partnerships with other members of the sector to provide mutual support and maintenance of essential services during a pandemic.

In certain instances, based on recommendations from local health authorities and organizations such as the World Health Organization and the Center for Disease Control, <<Company Name>> may find it necessary to impose non-punitive liberal leave on employees who may have been exposed to pandemic flu.

The Crisis Response Team will decide as to whether the office should remain open for business—the decision will be sent via email. If the office is closed then employees should work remotely until they are updated by the Crisis Response Team.

13.3.2 CRISIS TEAM SUGGESTED RESPONSIBILITIES / DUTIES

Depending on context, the Crisis Response Team should consider the following duties during and after a Level 3 event.

13.3.2.1 PRIMARY CRISIS MANAGER DUTIES

1. Contact board members, key officials and clients to explain the situation.
2. After the final damage is assessed, contact department managers/directors to request that their staff be called with further instructions (when to come in, where to meet, whether assistance is needed, etc.).
3. If there are casualties, contact the family of the victims within 24 hours to express sympathy and support.

13.3.2.2 DEPUTY CRISIS MANAGER DUTIES

Update staff via e-mail as needed.

13.3.2.3 LEGAL COORDINATOR DUTIES

1. On-call to answer any legal questions that might arise.
2. Document all interaction during the day, including: meetings, press conferences, etc.

13.3.2.4 ADMINISTRATIVE COORDINATOR DUTIES

1. If accessible, leave a voice message on the main telephone system.
2. Get phone lines in order. If needed, contact staff to assist in answering phones or helping with other administrative duties.

13.4 LEVEL 4: REPUTATIONAL CRISES

Level 4 crises are primarily reputational.

13.4.1 CRISIS TEAM RESPONSIBILITIES / DUTIES

The Crisis Response Team have the following duties during and after a Level 4 event.

13.4.1.1 PRIMARY CRISIS MANAGER DUTIES

1. Handle all correspondence with board members, key officials and clients.
2. Call an all staff meeting to inform employees about the situation and to impose rumor control policy.

13.4.1.2 DEPUTY CRISIS MANAGER DUTIES

1. Hold a meeting with management to discuss the situation.
2. Assist Crisis Communication Manager in answering employees' questions during all meetings.

13.4.1.3 COMMUNICATION COORDINATOR DUTIES

1. If appropriate, issue a statement about the negative coverage on <<Company Name>> website.
2. If appropriate, issue a news release.
3. Contact the media outlet that covered the story and provide our side.
4. Address all media concerns.
5. If needed, prepare the spokesperson for interviews or media briefing.
6. Track all media coverage and respond immediately to inaccurate information.

13.4.1.4 LEGAL COORDINATOR DUTIES

1. On-call to answer any legal questions that might arise.
2. Document all interaction during the day, including: meetings, press conferences, etc.

13.4.1.5 ADMINISTRATIVE COORDINATOR DUTIES

1. Get phone lines in order.
2. Prepare a statement to be addressed to the entire membership.

13.5 INCIDENTS NOT COVERED BY A CONTINGENCY PLAN

In the event of a crisis that doesn't have a contingency plan all members of the Crisis Response Team that are currently onsite, at <<Company Name>> headquarters based in <<Company City>>, are to immediately meet to prepare an appropriate response to the incident. If a Conference Room is available, it will serve as the Crisis Response Headquarters for all activities. If the <<Company Name>> office is not functional, the Crisis Response Team will meet at a to-be-determined alternate site, whether at a co-location or an alternate safe location.

All <<Company Name>> staff will be used as needed by the Crisis Response Team. Staff will remain on-call until needed or notified that their duties are no longer needed. Building exit procedures have been provided to all staff members in the case of an emergency. Walkthroughs have also been completed on a yearly basis. Exit doors are clearly marked and are easily accessible and free from and blockage.

14 SYSTEM MONITORING

<<Company Name>> has implemented and maintains procedures for:

1. Detecting an incident.
2. Regular monitoring of an incident.
3. Internal communication within the organization and receiving, documenting and responding to communication from interested parties.
4. Receiving, documenting and responding to any national or regional risk advisory system or equivalent.
5. Assuring availability of the means of communication during a disruptive incident.
6. Facilitating structured communication with emergency responders.
7. Recording of vital information about the incident, actions taken and decisions made, and the following shall also be considered and implemented where applicable:

- Alerting interested parties potentially impacted by an actual or impending disruptive incident.
- Assuring the interoperability of multiple responding organizations and personnel;
- Operation of a communications facility.

Ultimately, the decision to escalate an anomaly to an incident is in the purview of information security.

15 TRAINING, TESTING, AND REVIEW

15.1 TRAINING

Employees on an annual basis will be trained on and walked through the disaster recovery procedures. The evacuation plan and specific scenarios will be discussed and acted out. Employees will be shown the emergency exits, where the meeting spot is, work with the members of the Crisis Response Team and review the disaster recovery plan. This schedule is separate from this document and is maintained by the Crisis Response Team. The disaster recovery plan will also be reviewed by the Crisis Response team after the simulation exercises to add or remove what might help to strengthen the plan. All <<Company City>> employees are required to attend the mandatory training and a roster of those who complete the training will be recorded. Any employee that is unavailable for the training dates must attend a separate training as soon as they are onsite otherwise they will face discipline.

In the event of substantive or significant changes within the organization or to the environment in which it operates training should be reinitiated. The decision as to whether to reinitiate business continuity training will be made at the discretion of the Crisis Response Team.

15.2 TESTING

The purpose of testing is to ensure resiliency, recovery and preparedness of <<Company Name>>'s processes. Business continuity testing should minimize the risk of disruption of operations. Tests should be based on appropriate scenarios that are well planned with clearly defined aims and objectives—most importantly tests should be conducted against management metrics. The ultimate purpose of testing is continuous improvement, plans should be updated based on the results from testing.

15.2.1 TABLE TOP TESTING

<<Company Name>> will perform disaster recovery table top testing at least annually. The table top exercise should be based on disaster scenarios outlined by the Business Continuity and Disaster Recovery Policy. The objectives of the table top exercise is ensure that:

- Staff are aware of their responsibilities and duties.
- Staff training has been adequate.
- All necessary resources are available as detailed in the recovery plan.
- All supplies can be obtained as anticipated.
- The plan has is current and reflects current arrangements and procedures.
- Bottlenecks, uncertainties, and unreliable procedures are identified and resolved prior to any actual recovery incident.
- Senior management are comfortable that the plans will work as expected.

15.2.2 FAILOVER TESTING

<<Company Name>> will perform failover testing to a secondary backup location at least annually, or after any substantial change to <<Company Name>>'s production systems. During failover testing the disaster recovery technology will be tested for functionality, accessibility and recovery times. <<Company Name>> should perform failover testing using production systems.

15.2.3 BACKUP TESTING

<<Company Name>> will perform backup tests annually to ensure that it is possible to retrieve and back up data from a remote backup within the time stipulated by <<Company Name>>'s recovery point objective (RPO) and recovery time objective (RTO). Tests should be performed on primary and backup systems.

15.2.3.1 CALL TREE TESTING

Call tree testing must be performed annually to ensure that all numbers are correct and employees can be reached via multiple forms of communication.

15.3 POST INCIDENT ASSESSMENT

Post disaster recovery involves gathering all the information of what occurred during a disaster, the amount cost from the damage along with other information to plan and determine how <<Company Name>> can be more prepared in the future. The assessment will assist in improving the current disaster recovery program and will allow the Crisis Response Team to brief executive management and stakeholders in the company on how the disaster was handled, what the losses were. The organization shall retain appropriate documented information as evidence of the results. The post disaster report will contain the following data:

1. General description of the disaster
2. Areas Affected
3. Extent of Damage
4. Operational Impact
5. Plan for Recovery
6. Personnel Requirements
7. External Support Requirements
8. Estimated Time of Recovery

The document will be presented in the lessons learned meaning soon after the recovery is complete and the Disaster Recovery Plan will be updated accordingly—see Appendix D. Post Incident assessments will be stored in <<Company Name>>'s Ticket Management System.

16 INTERNAL AUDIT

<<Company Name>>'s ISMS Manager shall conduct internal audits at planned intervals to provide information on whether the business continuity management system:

1. Conforms to:
    0. the organization's own requirements for its business continuity management system,
    1. the requirements of this International Standard, and
2. Is effectively implemented and maintained.

Additionally, the organization should:

- Plan, establish, implement and maintain (an) audit program(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit program(s) shall take into consideration the importance of the processes concerned and the results of previous audits.
- Define the audit criteria and scope for each audit.
- Select auditors and conduct audits to ensure objectivity and the impartiality of the audit process.
- Ensure that the results of the audits are reported to relevant management.
- Retain documented information as evidence of the implementation of the audit program and the audit results.

The audit program, including any schedule, shall be based on the results of risk assessments of the organization's activities, and the results of previous audits. The audit procedures shall cover the scope, frequency, methodologies and competencies, as well as the responsibilities and requirements for conducting audits and reporting results.

The management responsible for the area being audited shall ensure that any necessary corrections and corrective actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification results.

17 MANAGEMENT REVIEW

The organization top management should annually review the organization’s Business Continuity Plans to ensure its continuing suitability, adequacy and effectiveness. The outputs of the management review shall include decisions related to continual improvement opportunities and the possible need for changes to the Business Continuity Plan.

18 CONTACT INFORMATION

Name of Security Program Owner

Title of Security Program Manager

Phone Number

Email

19 DOCUMENT RACI

Responsible	Assigned to do the work	Security Program Manager
Accountable	Final decision, ultimately answerable	ISM Governance Committee
Consulted	Consulted BEFORE an action or decision is taken (proactive)	Executive Management
Informed	Informed AFTER a decision or action has been taken (reactive)	Named Participants in this document Other parties affected by the change

20 LICENSE INFORMATION

APPENDIX A: REFERENCE LIST

- American National Standards Institute, “ISO/IEC 27001:2013, Information Security Management Systems.”
- American National Standards Institute, “ISO/IEC 27031:2011, Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity.”
- American National Standards Institute, “ISO 22302:2012.”

APPENDIX B: CONTACT LIST

EMPLOYEE PHONE NUMBERS

Emergency contact information for all employees is maintained in a separate repository that is provided to members of the Crisis Response Team.

FACILITIES AND UTILITIES CONTACT LIST

Name	Phone	Comments
AWS	Phone number available after case generated online using AWS credentials.	Account# ****************.
Acme Holdings (Primary)	555-555-3495	Victor Terrnova is our primary contact.
Acme Holdings (Secondary)	555-555-8903	George Olsen is our technology contact.

CONTACT LIST OF LOCAL AND NATIONAL AUTHORITIES

Name	Phone	Comments
Boston Police	617-343-4730	
Boston Fire	781-343-3550	
Federal Bureau of Investigation	617-742-5533	
Attorney General’s Office	617-727-2200	Office of the Attorney General One Ashburton Place Boston, MA 02108
Director of the Office Consumer Affairs and Business Regulations	617-973-8787	

21 APPENDIX C: BUSINESS CONTINUITY TASKS

Crisis Procedures	Level 1	Level 2	Level 3	Level 4
	INFORMATION SECURITY: Data Center Failure, Network Intruder, Data Breach, DDOS, Technical Disruption, Critical Equipment Failure,	**LOSS OF FACILITY: Fire, Structural Damage of the Office, Inclement Weather - Natural Disaster, Malicious Activity, Regional Disruption**	**Loss of Life, Pandemic**	**Reputational Crisis**

Primary Crisis Manager	Contact board members, key officials and clients to explain the situation	1. Contact all department managers to request that their staff be called and informed not to take appropriate action, e.g. evacuate, shelter in-place, etc. 2. Contact board members, key officials and clients to explain the situation. 3. If there are casualties, contact the family of the victims within 24 hours to express sympathy and support.	1. Contact board members, key officials and clients to explain the situation. 2. After the final damage is assessed, contact department managers/directors to request that their staff be called with further instructions (when to come in, where to meet, whether assistance is needed, etc.). 3. If there are casualties, contact the family of the victims within 24 hours to express sympathy and support.	1. Handle all correspondence with board members, key officials and clients. 2. Call an all staff meeting to inform employees about the situation and to impose rumor control policy.

Deputy Crisis Manager	Provide communication team with frequent on-site updates.	1. Provide Communication Team with frequent updates. 2. Address any public concerns with approved briefing information. 3. Provide on-site media and family with approved information and contacts.	Update staff via e-mail as needed.	1. Hold a meeting with management to discuss the situation. 2. Assist Crisis Communication Manager in answering employees' questions during all meetings.

Communication Coordinator	1. If appropriate, issue a news release. 2. If needed, prepare spokesperson for media briefing. 3. Address all media concerns. 4. Prepare statements. 5. If needed, coordinate press conference(s). 6. Track all media coverage with the assistance of other Corporate Communication staff and immediately respond to inaccurate information.	1. If needed, issue a news release. 2. If needed, prepare spokesperson for media briefing. 3. Address all media concerns. 4. Prepare statements. 5. If needed, coordinate press conference(s). Track all media coverage with the assistance of other Corporate Communication staff and immediately respond to inaccurate information.	Issue a statement about the negative coverage on the website, issue a news release, contact media outlets that covered the story and provide our side, address all media concerns, prepare the spokesperson for interviews or media briefing, track all media coverage and respond immediately to inaccurate information	1. If appropriate, issue a statement about the negative coverage on <<Company Name>> website. 2. If appropriate, issue a news release. 3. Contact the media outlet that covered the story and provide our side. 4. Address all media concerns. 5. If needed, prepare the spokesperson for interviews or media briefing. 6. Track all media coverage and respond immediately to inaccurate information.

Legal Coordinator	1. Call back-up counsel if needed. 2. Document all interaction during the day, including meetings, press conferences, etc.	1. If casualties, call the victims' emergency contacts. 2. Answer any questions or concerns from staff or family members. 3. Call back-up counsel if needed. 4. Document all interaction during the day, including meetings, press conferences, etc.	1. On-call to answer any legal questions that might arise. 2. Document all interaction during the day, including: meetings, press conferences, etc.	1. On-call to answer any legal questions that might arise. 2. Document all interaction during the day, including: meetings, press conferences, etc.
Administrator Coordinator	1. Work in support of Primary Crisis and IT Crisis Manager.	1. If accessible, leave a voice message on the main telephone system. 2. Get phone lines in order. If needed, contact staff to assist in answering phones or helping with other administrative duties (crowd control, tours, etc.).	1. If accessible, leave a voice message on the main telephone system. 2. Get phone lines in order. If needed, contact staff to assist in answering phones or helping with other administrative duties.	1. Get phone lines in order. 2. Prepare a statement to be addressed to the entire membership.

IT Crisis Manager	Determine the extent of the damage to the current systems, what data can be recovered and if new equipment needs to be purchased.	Determine the extent of the damage and if new equipment needs to be purchased.		

Communication Coordinator if Data Breach	If there is a data breach, prepare statements to the appropriate authorities and customers. Information should include: a. A detailed description of the nature and circumstances of the breach of security or unauthorized acquisition or use of personal information; b. The number of Massachusetts residents affected as of the time of notification; c. The steps already taken relative to the incident; d. Any steps intended to be taken relative to the incident after notification; and e. Information regarding whether law enforcement is engaged investigating the incident.			