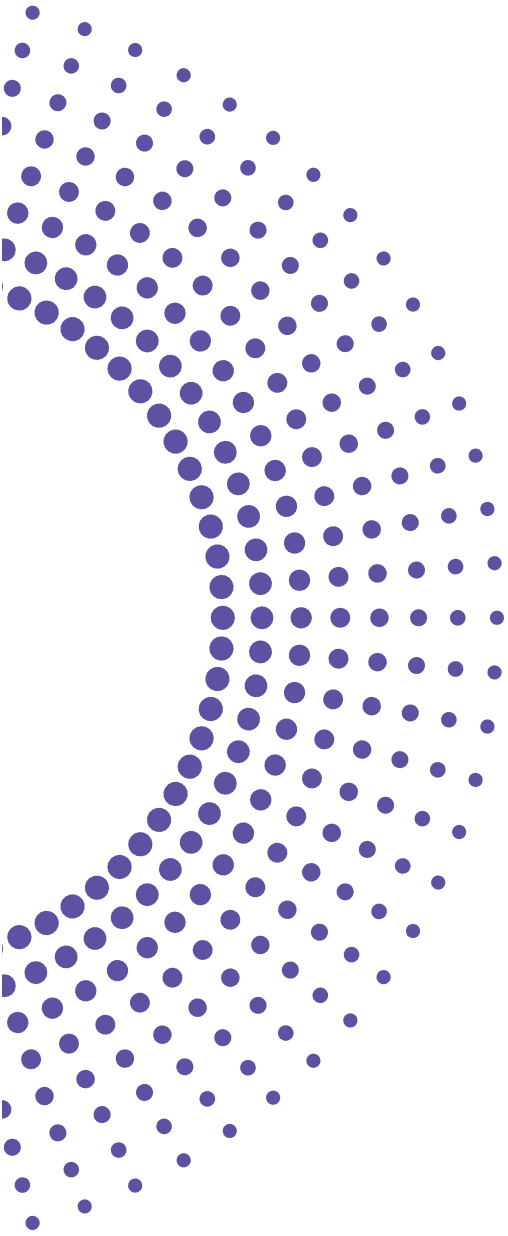

Business Continuity and Disaster Recovery Policies

September 2022

Policy

Salt (the “Company”) is to have a plan that is designed to ensure the continuity of its critical business functions and to minimize inconvenience and disruption of services to clients during disasters.

Responsibility

The Disaster Recovery (D/R) Officer is responsible for the implementation and monitoring of Salt’s Business Continuity and Disaster Recovery Policies and Procedures (“BC/DR Policies”), including associated practices, disclosures and recordkeeping. The D/R Officer may delegate responsibility for the performance of these activities (provided that it maintains records evidencing individual delegates) but oversight and ultimate responsibility remain with the D/R Officer.

Procedure

The Company has adopted various procedures to implement the BC/DR Policies and reviews to monitor and ensure that they are observed, implemented properly and amended or updated, as appropriate. The procedures are as follows:

DISASTER RECOVERY PLAN

The Company recognizes its operational dependency on computer systems, networks, database services, Internet, e-mail, telephone and fax services, electrical power and other essential items and the potential loss of revenue and operational control that may occur in the event of a disaster. Salt has authorized the preparation, implementation and maintenance of this comprehensive Disaster Recovery Plan. The intent of this Plan is to provide a written and tested plan directing officers and staff to take certain actions in the event of an interruption in continuous services resulting from an unplanned or unexpected disaster.

This Business Continuity and Disaster Recovery Plan is designed to recover from the "worst case" destruction of Salt’s operating environment. The "worst case" destruction assumes the loss of the total facility, supporting infrastructures (e.g., power grids, telephone switching centers, microwave towers, and cell and wireless transmission sites near the location of Company), and the incapacity of key personnel.

These procedures describe Salt’s overall approach to disaster preparation and recovery. They are designed to minimize loss and ensure the continuity of the critical business functions of the Company in the event of a disaster.

DISASTER RECOVERY (D/R) OFFICER

The Company shall have in place a Disaster Recovery (D/R) Officer who carries out these procedures and provides for a coordinated disaster recovery response. Key personnel have been assigned certain roles and are responsible for managing resources, gathering and analyzing information and making decisions during an emergency.

The Disaster Recovery (D/R) Officer shall have the following responsibilities:

- Develop and maintain this Disaster Recovery Plan;
- Procure the necessary supplies, equipment and systems to implement the Disaster Recovery Plan and to support disaster recovery in the event of a disaster;
- Conduct training drills; and
- Keep current on threats and identify potential disasters that may disrupt the operations of the Company.

IDENTIFYING POTENTIAL DISASTERS

The D/R Officer shall meet periodically with the Company's senior management to discuss types of potential disruptions to the operations of Company and to plan how it will operate during, and recover from, those disruptions. Potential disasters and disruptions include:

- Power Outage
- Building Fire
- Virus, Cyber or Other Attacks on Data
- Severe Inclement Weather
- Flood
- Earthquake
- Bomb Threat
- Hazardous Materials/Biological Event
- Terrorist Attack

DISASTER RESPONSE

In the event of a disaster or other event that causes a severe disruption in the operations of the Company, the following steps shall be taken:

- Officers of the Company who become aware of the disaster shall contact the D/R Officer, and, if the D/R Officer is unavailable, shall contact another senior officer of Company.
- The D/R Officer, or whoever was notified of the incident, shall contact the CEO and members of the senior management and call them together if, in their judgment, it is necessary to implement the Disaster Recovery Plan.
- The D/R Officer shall gather critical information about the disaster and its impact on the operations of Company. Such information may include:
    - What are the unresolved issues?
    - What is needed and where is it needed?
    - What progress has the Company made towards implementing the Disaster Recovery Plan and resuming normal operations?
    - Who is working on what and where are they?
- The D/R Officer shall monitor:
    - Personnel
    - Health and safety
    - Computer operations
    - Communication
    - Equipment
    - Disaster situation
- The D/R Officer shall determine appropriate response strategies.
- The D/R Officer shall activate resources.
- The D/R Officer shall oversee activities related to disaster response and recovery.
- The D/R Officer shall declare, at the appropriate time, the incident is over and that Firm and its personnel should return to normal business operations.

CRITICAL BUSINESS FUNCTIONS

The Company has identified the following as being critical to its operations and developed the following back-up plans to keep them functioning during an emergency or disruption:

BUILDING
If the office housing the primary operations of the Company is unable to function and continue normal business activities, employees will access systems required to maintain critical business activities remotely from

home or at a back-up location pre-designated by the D/R Officer and key personnel will relocate to that location. Once logged in remotely or at the location, all systems are automatically accessible by essential personnel to carry on operations at the new location.

DATA/RECORDS
The Company stores all data about clients, client transactions, the Company and other operations on servers, hard drives or other storage medium located in one or more data centers maintained by commercial cloud-based providers with local redundancy. The Company maintains software for data intake and analysis, generation of analytics, delivery of information to third-parties, and other operations to support its business. It is essential that this data and software is preserved and accessible. All virtual machines, files, databases, or other electronic media are backed up at least daily by the cloud provider(s) and are accessible remotely with proper credentials.

Salt employs firewalls to ensure data is only accessed by individuals with a need to know and with the correct access privileges and where deemed necessary, encrypts data.

Salt has installed an access control security system that allows only authorized personnel to access data.

CLIENT COMMUNICATION/CUSTOMER SERVICE
The Company communicates to its clients by telephone, electronic mail, and regular mail. Any and all methods of communications may be unavailable for periods of time. The Company will take the necessary steps to implement an alternative communication system in the event of a disaster.

The Company has a call forwarding system for its telephone lines. If telephone service is interrupted, calls will be forwarded to another location as requested of the telecommunications provider and Company staff can access alternate devices to receive calls.

VENDORS/TRANSACTION PROCESSING
The Company has a number of relationships with vendors that supply services that are critical to its business operations. The D/R Officer shall maintain an online and printed copy of emergency phone numbers at contacts of all critical vendors. The D/R Officer shall coordinate with vendors to determine procedures in the event there is a disaster that impacts the delivery of services to the Company. Such contingency planning shall cover a disaster at Salt, the vendor or both.

Salt will continually monitor external dependencies on third party service providers.