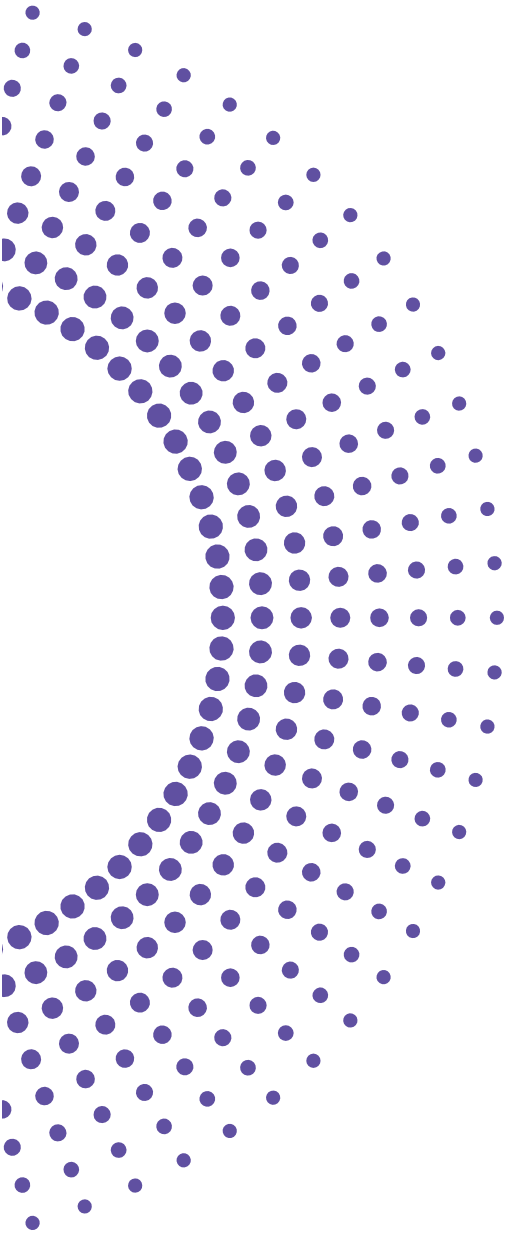

# Cybersecurity Policies & Procedures

March 2022

Version History

| No. | Date | Author | Comments |
|---|---|---|---|
| 1.0 | 3/8/2022 | E.Bae | Initial |
| | | | |
| | | | |

## Policy

Salt Financial LLC's ("Salt's") policy is to implement procedures designed to ensure the confidentiality, integrity, and availability of Salt's proprietary and nonpublic personal and business information and Salt's electronic systems.

## Background & Description

Salt's business partners expect that Salt will assess its ability to protect its proprietary and nonpublic information and electronic systems, take steps to mitigate the risk of loss of such information or access to its electronic systems, and be able to perform critical functions to fulfill regulatory requirements and contractual obligations.

## Responsibility

Salt will designate a Cybersecurity Officer, who may be a current Salt employee, officer, or contractor, to oversee the development, implementation and monitoring of the Salt's cybersecurity controls and policies, including associated practices, disclosures and recordkeeping. The Cybersecurity Officer may delegate responsibility for the performance of these activities (provided that it maintains records evidencing individual delegations).

## Procedures

Salt has adopted the following procedures to implement the firm's Cybersecurity policy and reviews to monitor and ensure that the firm's policy is observed, implemented properly and amended or updated, as appropriate.

The procedures implemented and maintained by the Cybersecurity Officer include the following:

- Safeguards for Confidential Information. All employees have a duty to protect Salt's confidential information. Employees shall take care not to accidentally disseminate confidential data and shall take precautions not to lose electronic devices, storage media, and hardcopy documents that contain confidential data.

- Passwords. Passwords act as an access control measure against inappropriate activity. Employees must use secure and unique passwords and comply with system-enforced expiration and complexity policies. Passwords must not be revealed, shared, posted, or stored in a manner that makes them easily available to others (including being sent in clear text messages). In particular, passwords must not be emailed or stored in electronic files.

- Anti-Virus and Anti-Malware Software. Salt will maintain appropriate technical cybersecurity protection, including anti-virus and anti-malware software, firewalls. and data loss prevention software. All Salt employees, agents, and contractors must have anti-virus software on their company-

issued computers or laptops and home computers used for business purposes. For data and network services provided by external cloud computing providers, Salt will use anti-virus and anti-malware features provided by the external providers.

- Secure Workstations. All Salt employees, agents, and contractors must shut down or lock their computers when they leave the office for an extended period of time. In addition, lockouts to employee workstations will be system-enforced.

- Reporting Security Incidents and Violations. Salt employees must immediately report to the Cybersecurity Officer any security incidents and violations, including the theft, loss, or unauthorized access to any nonpublic or proprietary personal or business information or any device containing any such information, such as work-related emails.

- Storage of Confidential Data. The storage of nonpublic or proprietary personal or business information on any removable or mobile media is prohibited.

- Access Requests. Salt employees must forward to the Cybersecurity Officer any requests from third parties for independent access to Salt's networks or proprietary data. Only the Chief Executive Officer or Cybersecurity Officer may grant such access requests.

- Inventory. Salt will maintain an inventory of Salt's computers, system hardware, and other IT devices. Salt will also inventory software applications used by Salt.

- Monitoring. Salt will monitor for unauthorized devices and individuals accessing Salt's networks, computers, electronic devices, and data.

- Patch Management. Salt will ensure that software patches and updates are being applied in a timely manner and that patches for critical vulnerabilities are made on an expedited basis.

- Penetration Testing. Salt will ensure that likely types of attack are evaluated, including through penetration testing and vulnerability scans.

- Testing Equipment and Software. Salt will periodically conduct tests to confirm that hardware, software, operating systems and network infrastructure continue to operate according to their standardized secure configurations.

- New Software and Applications. New software applications must be evaluated for cybersecurity and other risks prior to implementation. Employees shall not use software applications to perform their duties for Salt that have not been approved by the Cybersecurity Officer.

- Terminating Network Access. Salt must promptly disable access for any terminated employees, agents, or contractors and promptly collect all firm distributed hardware from such persons.

- Third Party Service Provider Risk Management. Salt will establish a program to assess third-party service providers for cybersecurity risks, including a review of contract terms, conducting diligence on third-party service providers' cybersecurity programs and capabilities to respond to cybersecurity attacks and cybersecurity protections, requiring notice of cybersecurity incidents affecting the third-party serviced providers and any data provided to them by Salt, and a review of the third-party service providers' internal cybersecurity testing and training.

- Access Controls. Salt will establish access controls to various systems and data via management of user credentials, authentication and authorization methods, firewalls and/or perimeter defenses, tiered access to sensitive information and network resources, network segregation, and system hardening. Users will only be granted access to electronic systems and data that are necessary to perform their roles and responsibilities.

- Encryption. Salt will consider implementing data encryption, where appropriate.

- Data Loss Prevention. Salt will protecting against the loss or exfiltration of sensitive data (including nonpublic personal and business information) by prohibiting the use of removable storage media and monitoring technology systems for unauthorized intrusions, the loss or exfiltration of sensitive data, or other unusual events.

- Data Backups. Salt will maintain backups of its systems and data and will periodically test its ability to restore critical data and software in a timely manner.

- Physical Security. Physical access to Salt's offices requires a key. Building security requires the check-in of visitors at reception after which access is granted. Employees are issued a building pass to gain access at the lobby and the office upstairs. Upon termination, an employee is required to turn over their office key. Visitors must be accompanied by authorized personnel who are responsible for them.

- Reporting Security Violations. All employees are responsible for ensuring the ongoing confidentiality, integrity, and availability of systems and information within the firm. If a violation of policy is detected, employees are obliged to report it to the Cybersecurity Officer immediately.

- Multi-Factor Authentication. Multi-factor authentication must be enabled for all applicable cloud applications and remote access to Salt systems and accounts, where possible.

- Wireless Network (Wi-Fi) Communications. The business WiFi network utilized by Salt to conduct its business shall only be accessible to employees with an appropriate access key. Personal devices can be connected to a guest network when properly segregated. All traffic that originates on the guest network is separated from the business network utilized by Salt.

- Acceptable Use. The primary purpose of Salt information assets (including but not limited to computer systems, software, storage media, communications systems and accounts providing email and Internet access) is to support the ongoing operation of Salt. Under no circumstances are personnel authorized or permitted to engage in any illegal activity (as defined by local, state, or federal law) while using Salt information assets.

- Clean Desk. Employees must use reasonable care to keep all paper copies of confidential and proprietary information out of view from persons who are not authorized to have to access to such information. Similarly, employees must take care to ensure that confidential and proprietary information on computers is not visible to persons who are not authorized to have access to such information.

- Secure Data and Electronic Device Disposal. At all equipment's end-of-life, sensitive data must be properly erased, destroyed, or as otherwise made unreadable. This is to ensure that all appropriate legal measures are taken to comply with software license agreements, non-disclosure agreements, and to keep critical and/or confidential information (including personal data) safeguarded. Similarly, hardcopy documents containing confidential information must be disposed or destroyed of in such a way as to make them unreadable to others, such as by shredding.

## Cloud Computing Providers

Due Salt's limited size and staffing, Salt uses large outside vendors, such as Microsoft Azure, to provide cloud computing and data management services. Salt relies in part on the robust cybersecurity programs of these providers to ensure the confidentiality, integrity, and availability of its systems and data. Salt periodically reviews the security configurations and features of its accounts with these providers to ensure that Salt's data and systems are protected.

## Assessment

On at least an annual basis the Cybersecurity Officer, along with its IT provider, will perform a cybersecurity assessment. The Cybersecurity Officer will supply senior management with the results of this review. The periodic assessment will consider the:

- nature, sensitivity and location of information that the firm collects, processes and/or stores, and the technology systems it uses;

- internal and external cybersecurity threats to and vulnerabilities of the firm's information and technology systems;
- security controls and processes currently in place;
- impact should the information or technology systems become compromised; and
- effectiveness of the governance structure for the management of cybersecurity risk.

## Email and Messaging

Employees should only use the email accounts provided by Salt for all company business conducted via email. All business-related electronic communication must take place via Salt's email system. If employees use Salt's email accounts for occasional personal emails, each employee should be aware that all such emails are subject to review and disclosure.

Employees should be aware that all Salt emails and communications are the company's property, may be retained indefinitely, are subject to periodic review by Salt or its agents (*e.g.* attorneys), and may be subject to review by regulatory authorities. Employees must acknowledge that Salt and its authorized agents have the right to access, obtain, and review all emails, including personal emails that users send or receive through the company's electronic resources. Employees expressly consent to such monitoring and review of all emails by Salt and/or its authorized agents.

Salt reserves the right to block certain email messages and attachments to protect Salt's infrastructure from malicious attack attempts. Users should not open attachments, click links, execute macros, or download files from unknown or suspicious sources.

Users will be kept aware of general indicators of malicious content through periodic training. When an inbound email has attachments, employees must verify that:

- It comes from an individual that appears legitimate
- The format/content/naming is as expected
- It does not look odd with unusual spelling or characters

## Training

The Cybersecurity Officer will ensure that cybersecurity training is conducted on an ongoing basis, which includes educating all Salt employees, agents, and contractors how to identify suspicious emails and phishing attempts and how to respond to a cybersecurity event. The training, which will be given to Supervised Persons initially upon hire and periodically thereafter, will be documented including the material covered, attendee list, and attestations of receipt of the training and the Salt's Cybersecurity Policy.

## Oversight of Key Service Providers

On at least an annual basis, the Cybersecurity Officer shall obtain reports (SOC 2 Report, or equivalent information security certification, Business Continuity Report) from "Key Service Providers," which are service provides that have access to Salt's electronic systems or confidential personal and business data.

The Cybersecurity Officer shall review the reports annually for purposes of ensuring that Key Service Providers have systems in place to address alternate arrangements for the handling of data, data processing, communications systems; and office and staffing plans in the event of a business disruption.

The Cybersecurity Officer shall also review the reports to determine whether the Key Service Providers have systems and procedures in place designed to ensure the protection of proprietary and nonpublic personal information stored on their electronic systems and to protect the firm in the event of a cybersecurity attack.

## Incident Response Plan

This incident response plan ("IRP") governs Salt's general response, documentation and reporting of network and computer-based IT security incidents (*i.e.*, cybersecurity incidents), such as theft, intrusion, misuse of data, denial of service, and unauthorized access or loss of personally identifiable information.

The IRP defines what constitutes a security incident at Salt and outlines the incident response phases. The IRP will define areas of responsibility and establish procedures for handling various cybersecurity incidents.

In the event of an incident, Salt will reach out to its relevant service providers that may assist in handling the incident, including, as appropriate, cybersecurity forensic experts, law firms, compliance consultants, and insurers.

Purpose. The purpose of the IRP is to:

- Protect the confidentiality, integrity and availability of Salt's proprietary information, to prevent loss of service and to comply with federal and state regulatory requirements;
- Mitigate the effects caused by such a security incident;
- Protect Salt's assets from future unauthorized access, use or damage; and
- Ensure that recovery from disruption of services is minimal and that data integrity and recovery of lost or corrupted data following an incident remain a priority.

Scope. This IRP applies to employees, contractors, consultants, temporaries, and other workers at Salt, including all personnel affiliated with third party service providers. This policy also applies to all equipment that is owned or leased by Salt.

Authority. The duties of Salt's Cybersecurity Officer include:

- Responsibility for the development, oversight and maintenance of the IRP and related procedures.
- The establishment of a Security Incident Response Team, which may include third party vendors, appropriate to respond to a specific incident, centralize and coordinate initiatives and communications.

Events and Incidents

- For the purposes of the IRP, an **event** is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt.
- The IRP events those that are computer security related, not those caused by natural disasters, power failures, etc.
- For the purposes of this policy, a computer security **incident** is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
- Security incidents include but are not limited to the following:
    - Loss of confidential information due to data theft;
    - Compromise of information integrity due to data damage/unauthorized modification;
    - Theft or damage of IT assets such as computers, storage devices, and printers;
    - Denial of service;
    - Misuse of services, information, or assets;
    - Infection of systems by unauthorized or hostile software;
    - A significant attempt at unauthorized access to Salt's data or systems;
    - Unauthorized changes to organizational hardware, software, or configuration;
    - Reports of unusual system behavior; and
    - Responses to intrusion detection alarms.

Incident Response Reporting

- Any employee of Salt, individual or outside firm may report a real or suspected security incident.
- The Cybersecurity Officer will declare that there is a security incident under investigation.
- Once declared, the Cybersecurity Officer will use standard internal procedures to log and track the security incident and as appropriate, and take steps to investigate, escalate, and remediate the incident.
- Salt will include a report of any security incidents or violations as part of any periodic cybersecurity assessments prepared.

Communication and Notification

- If the Cybersecurity Officer determines that a serious security breach has occurred that may have compromised Salt's sensitive assets, the Cybersecurity Officer shall initiate the communication plan described herein. A "serious" security breach will include the unauthorized access to or compromise of Salt's systems and data, including personal data.

- All affected Salt partners, clients, and other business affiliates will be notified of a confirmed breach if required by federal/state laws and regulations.
- If required by law, the breach notification will provide all information as required by law, which include, but need not be limited to, a brief description of the security breach, a contact for inquiries, and helpful references to individuals regarding identity theft and fraud (if applicable).
- Salt will notify appropriate regulators of cybersecurity incidents and events if required by state or federal law.
- Any press or media inquiries regarding the security breach should be directed to the Cybersecurity Officer. Under no circumstances should employees take it upon themselves to engage in any communications with the press or media regarding any suspected or actual cybersecurity breaches.
- The Cybersecurity Officer will determine if law enforcement should be informed. It is Salt's policy to cooperate fully with law enforcement in the investigation of any cybersecurity breach and Salt expects the same level of cooperation from its employees, contractors, consultants, temporary workers and any other parties with access to its systems who may have information that can assist in identifying who is responsible and/or mitigating/remediating the effects of the attack. The same will be true if the Cybersecurity Officer determines it is necessary to utilize Salt's retained external forensic services.

Incident Response Procedures. The Cybersecurity Officer should be available for anyone who discovers or suspects that an incident involving Salt has occurred. The Cybersecurity Officer will then handle the incident. The Cybersecurity Officer's role is to analyze the incident data, determine the impact of the incident, and act appropriately to limit the damage and restore normal services. The Cybersecurity Officer's success depends on the participation and cooperation of individuals throughout Salt. If necessary, the Cybersecurity Officer will retain outside professionals to assist with the implementation of the IRP in the event of an incident.

Incident Response Process. The incident response process has 4 Main phases –

- Preparation: The Cybersecurity Officer will ensure that incidents are appropriately documented, logged/tracked and archived.
- Detection and Analysis: The Cybersecurity Officer will determine the nature and severity of the incident.
    - Containment, Eradication and Recovery: The Cybersecurity Officer shall conduct a further investigation of the incident. After the investigation, the Cybersecurity Officer will take steps to eradicate the threat and restore services. Containment procedures should ensure, as feasible under the circumstances, that evidence is preserved for forensic analysis and that the chain of custody for evidence is documented.
- Post-Incident Report: After the incident is contained and mitigated, the Cybersecurity Officer shall prepare a report for all serious incidents that

identifies (i) what happened, (ii) what steps were taken to remedy the incident, and (iii) what lessons were learned so that Salt's policies and procedures may be improved.

Storage of Incident File and Evidence

- All evidence, logs, and data associated with the incident should be grouped together and placed in limited access, secure storage.
- Access to the storage should be limited to personnel on a need-to-know basis.
- If evidence is turned over to law enforcement, the Cybersecurity Officer shall create an itemized inventory of all the items, verify the inventory with the law enforcement representative, and have the representative sign and date the inventory list and make a similar entry in the evidence log.
- If the original records are turned over to an entity outside of Salt, an appropriate entry should be made and maintained by Salt in the evidence log.