CYBERSECURITY AND PERSONAL INFORMATION PROTECTION POLICY

Updated September 2023

Overview

This policy applies to all Coastal ("Coastal" or "Firm" includes Coastal Equities, Inc., Coastal Investment Advisors, Inc. and their parents, affiliates, and subsidiaries) employees, registered personnel and associated persons conducting business in the Home Office or a branch, as well as persons working from a home office or other office of convenience (together defined as "Personnel"). The purpose for this policy is to establish the general framework for governance of its Personnel in the field. This Policy also applies to the Home Office except to the extent it may conflict with the Policies of the Home Office Addendum, provided only to Home Office Personnel.

Personnel

All registered representatives/investment adviser representatives must pass a background check and are fingerprinted. All other personnel with access, or potential access, to customer personally identifiable information ("PII", includes name, d/o/b, SSN, etc.) or other information assets ("Assets") which are proprietary to the Firm (commission schedules, vendor lists, customer lists, etc.) must be identified to and approved by Coastal prior to working at the branch with access to PII and Assets. Such individuals must also pass a background check and be fingerprinted.

The on-site Branch Manager, or Person in Charge of the branch, is responsible for enforcing this Cybersecurity and Personal Information Protection Policy in the field.

Clean Desk Policy

A clean desk policy can be an import tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, representatives, our customers and our vendors is secure in locked areas and out of sight. A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

a. Personnel are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
b. Computer workstations must be locked when workspace is unoccupied. (In Windows there is a 'Lock' option on the Start menu.)
c. Computer workstations must be shut completely down at the end of the work day.
d. Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
e. File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
f. Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

g. Cell phones and tablets with Restricted or Sensitive information must be locked when not in use or when not attended.
h. Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
i. Upon disposal, Restricted and/or Sensitive documents should be shredded or placed in locked confidential disposal bins.
j. Whiteboards containing Restricted and/or Sensitive information should be erased.
k. Physically lock away portable computing devices such as laptops and tablets.
l. Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer. Mass storage devices may not be removed from the office premises without the express permission of Compliance.
m. All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

Document Storage

Paper files must be maintained in locked file cabinets, locked filing room, or closet.

Access to Personal Information

Only registered persons and Personnel approved by Coastal are permitted to have access to PII or Assets. Unapproved individuals and contractors occupying or using the premises must not be permitted to access PII or Assets of the firm. Limit keys only to persons permitted to access the PII or Assets. Compliance with the Clean Desk Policy will also help mitigate the risk of unauthorized persons improperly accessing PII or Assets.

Shredding/Document Destruction

All documents containing PII or Asset information must be maintained for the requisite books and records period (typically six years). After the expiration of the applicable time period documents may be destroyed by either shredding or incinerating the documents. Please provide notice to the Home Office of your intent to utilize the vendor at least thirty (30) days prior to use so the firm may review the vendor. If you have conducted your own Due Diligence on the vendor, please forward a copy to Compliance in order to expedite your request to use the vendor.

Shared Office Space

Arrangements to share office space with third parties must be approved by Coastal prior to engaging in sharing the space. In the event an arrangement is approved, great care must be taken to observe these policies and procedures. Systems such as filing cabinets, copiers (with hard drives or network connectivity), internet, wi-fi, and physical networks may not be shared with the entity due to the risk of inadvertent disclosure of PII or Assets. Such systems must be locked and password protected at all times.

Cybersecurity

Inventory of Assets and Vendors

You must maintain an inventory of all assets used to access PII or Assets and report this to the Firm. The Firm uses Entreda, a software application installed on each of your devices or computers, to catalogue and monitor all devices used to connect to PII or Assets of the Firm, and registration is required by the Field. *See below for more information about Entreda.*

Adding/Removing Devices: Please be sure to unregister devices no longer used by the branch after all PII and Assets have been deleted from the storage systems of the device. *See Retirement of Equipment Containing Data below*. Please contact Dan Rhoads with questions at drhoads@coastal-one.com. Likewise, please be sure to register new devices with Entreda prior to use. Any devices discovered accessing PII or Assets of the Firm which are not registered through Entreda will result in discipline of the responsible Personnel and Branch Manager/PIC.

Vendors: You must also inventory all systems and vendors used in your practice which maintain, store, or have access to PII or Assets. You must obtain written approval by Compliance to utilize software in your practice not already Whitelisted by the Firm.

You must perform due diligence before engaging a vendor, including technology consultants, given that they will quite often have access to PII, or could potentially install malicious software on your systems when they have access. At a minimum, you should review the vendor's: Privacy Statement, Terms of Use Statement on their website, Disaster Recovery or Business Continuity Plan, the identity of any cloud services utilized and a SOC 1 or SOC 2 Report if available. This review should be documented and maintained in a vendor due diligence file at the branch.

Access Management

Where possible, limit access of persons in your office on a "need to know" basis. This will limit the access of wrong-doers in the event one individual's access credentials are compromised, and limit the exposure of a breach.

Laptops and Other Portable Devices Used by Personnel

Personnel who use laptops or other mobile devices for Firm business are responsible for the security of the device and the information contained on it. Serious security breaches can occur if a device containing or capable of accessing confidential information is lost or stolen.

Personnel who use laptops for company business (including but not limited to storage or access to PII or Assets) are required to comply with the following requirements:

- All laptops, whether company issued or property of an associated person, must be password protected and encrypted, and registered with Entreda.
- When traveling, laptops must be kept on-person or locked up unless tracking software has been installed
- Mobile devices must be password protected or have a "lock" feature enabled.
- Mobile devices must not be left unattended, even on desks. These devices should be treated like cash, not to be left out in the open.
- When travelling, mobile devices must be carried in carry-on luggage and not in checked luggage
- The loss of a mobile device must be immediately reported to Compliance.

Prohibited Downloading. All persons are prohibited from using portable devices such as USB key drives, MP3 players, mobile phones, and other devices for downloading information.

Control of Access. Authorized personnel are issued passwords to access systems and records; these passwords are periodically changed. Accounts and Passwords are disabled when Personnel terminate or are no longer an authorized person.

Encryption of Data. Data regarding private customer information transmitted to laptops or remote devices will be encrypted. Such data stored on laptops and other remote devices will also be encrypted.

Retirement of Equipment Containing Data. Computers or other data-retaining equipment that will be disposed of will be subject to clearing of hard drives and other repositories of data prior to disposal. If a computer will be re-assigned to someone who is not authorized to view data stored on that computer, the hard drive will be cleared prior to reassignment. Flash drives and other portable data devices that will no longer be used or will be reassigned will be destroyed or cleared of all data prior to disposal or re-use.

Data Storage

Electronic data storage must be "WORM" (Write Once Read Many times) compliant, and of course, secure. If you use a local server or hard drive to store data, the server or hard drive must be encrypted and password protected. Cloud storage systems may or may not be compliant. Please obtain approval from Compliance prior to engaging a cloud service to store PII or Assets by providing your due diligence addressing the above concerns with your request to Compliance.

Access to Customer Information Via Wi-Fi. Because of risk of unauthorized access by outside parties and the difficulty of ensuring the security of wireless connections to the Internet, associated persons are not permitted to use wireless fidelity (Wi-Fi) to access customer account information, unless:

- the associated person is working on Coastal premises (Home Office or branch); or
- the associated person has installed Firm-required firewalls or other protections and has prior approval from Compliance to use Wi-Fi for Firm business.

Compliance

The Branch Manager or Person-In-Charge of the branch will monitor compliance to this policy through various methods, including but not limited to, periodic walk-throughs, internal and external audits, and feedback from staff. Coastal also monitors compliance to this policy during branch examinations. *All breaches of policy must be reported to Compliance immediately. All incidents and PII breaches must be reported to Compliance immediately.*

Exceptions

Any exception to the policy must be approved by Compliance in advance.

Non-Compliance

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Additional Information

Incident Response and Reporting

Please refer to Appendix 1 at the end of this Manual. All incidents should be reported to the Home Office immediately, and the incident response should be coordinated with personnel at the Home Office. Branches should also create their own disaster recovery plan in the event of data loss, for example. A default Disaster Recovery Plan is attached for reference. This Plan should be tailored for your office's particular circumstances if needed.

Personnel Termination

In addition to the return of desk and office keys, Personnel should immediately be removed from all entitlements to web and network access to firm systems, and all mobile devices should be returned to the office, or wiped of all PII and Assets if the device was a personal device. Employees who wish to use personal devices must be alerted by the Branch Manager or PIC upon first use that the device will be wiped upon termination. Branch Managers and other Registered Persons may maintain data concerning their clients only unless it would otherwise cause a breach of the Policies and Procedures of the Firm.

ENTREDA

Entreda is an enterprise solution used by Coastal to monitor its Personnel's electronic devices in the field, as well as in the Home Office. Entreda uses an application which runs in the background on your devices and monitors various security risks on the device. The application then generates a score and reports this score to the Home Office, as well as to the user.

The score is based on reviews of firewall protection, file sharing entitlements, anti-virus, disk encryption, password strength, password expiration, anti-spyware, security update settings, and wi-fi encryption. A combination of the above factors generates a score. This score varies from 0 to 800 and graded.

Devices with a Grade A are in compliance. Grades B or C require the user to remediate the issues within thirty (30) days of notice and the user may receive communication from the Home Office concerning the issue. Devices graded C or D require remediation within seven (7) business days, and Grade F will require immediate remediation. Failure to remediate will result in immediate removal of access to Coastal systems until remediation is completed, and possible discipline by the firm.

APPENDIX

---

1. Data Breach Incident Response Policy
2. Incident Report Form
3. US Law Enforcement Contacts
4. Password Protection and Construction Guidelines
5. Acceptable Use Policy

APPENDIX 1

Data Breach Incident Response Policy

Purpose and Scope

This Data Breach Incident Response Plan provides the plans, procedures and guidance for the handling of data breach events at our branch offices, or via any of your servers or mobile devices.

The plan encompasses procedures on incident response engagement and how the incident response team will communicate with the rest of the organization, with other organizations, with law enforcement and provides guidance on federal and local reporting notifications processes.

As of March 30, 2019, management has designated Dan Rhoads as the primary party responsible for the Plan, procedures and updates.

The information contained in this plan is current as of September 1, 2023, and may be updated on annual basis.

Incident Response Plan

An incident response plan is necessary to clarify the roles and responsibilities of Coastal employees and registered persons so Coastal can quickly mitigate risks, reduce the organization's attack surface, contain and remediate an attack, and minimize overall potential losses.

Branch incident response team: Branches should designate at least one person at your branch to be responsible for incident response, and to correspond with the Coastal incident response team when needed.

The Coastal Incident Response Team includes:

- Dan Rhoads
- Ken Fischer

IT includes Coastal's IT department, the branch IT department, or where a branch has no IT department, the Branch Manager, Person in Charge, or his/her respective designee.

Identification of System Criticality and Order of Restoration Priority

Coastal primarily relies upon its clearing firm for trading activity and account maintenance. Internal systems concerning its back office operations are located on an internal server (NAS), cloud storage provided by Citrix, and local workstations, with backups to Amazon Glacier and Backblaze respectively.

Coastal's registered persons and their staff are independent contractors, and therefore all branch systems are maintained locally, with the exception of clearing firm systems. When local branch systems are compromised, the branch should refer to the Coastal Business Continuity Plan for instructions concerning trading activity and account maintenance and its own Business Continuity Plan when applicable for restoration priority of its local systems.

Incident Detection and Identification Guidelines

The table below identifies a list of some common security incidents which may require incident response and the recommended actions and reporting requirements for Coastal.

Table 1 - Incident Classification Types

SECURITY EVENT TYPE	PRIORITY	RECOMMENDED ACTION	REPORTING REQUIREMENTS
Port Scanning Activity	Low	Temporarily shun offending IP address for 15-30 minutes.	N/A
Phishing Attack	Low	Alert staff. Block emails from offending domain.	N/A

Spear Phishing Attack	Low	Alert staff. Document activity.	N/A
Internal Policy Violation	Med	Notify offending party. Determine if action taken was intentional or an indicator of compromise. Document and take action if necessary.	N/A
Web Defacement	Med	Take down website temporarily. Review logs to determine how access was achieved. Perform comparative code analysis to determine modifications. Update all plugins and change all passwords.	Depending on type of disruption, notification may be necessary.
Identification of Malicious Code or Malware Infection	High	Review logs and determine if activity is limited to a single	Disclosure may be necessary if a breach has occurred.

		workstation or is widespread. If widespread, engage forensics professional to determine extent of compromise.	
Ransomware or malicious encryption	High	Take system offline to prevent further spread of malicious encryption. Wipe system and restore from backup.	N/A

External Unauthorized Access	High	Engage forensics professional to determine extent of compromise. Do not turn off/disconnect system until receiving instructions from forensics professional.	Disclosure may be necessary if a breach has occurred.
Insider Unauthorized Access and Use	High	Engage forensics professional to determine extent of compromise. Do not turn off/disconnect system(s) until receiving instructions for forensics professional.	Disclosure may be necessary if a breach has occurred.
Compromised User Credentials	High	Engage forensics professional to determine extent of compromise. Do not turn off/disconnect system(s) until receiving instructions for forensics professional.	Disclosure may be necessary if a breach has occurred.
Exploitation and Installation	High	Engage forensics professional to determine extent of compromise. Do not turn off/disconnect system(s) until receiving instructions for forensics professional.	Disclosure may be necessary if a breach has occurred.

Unauthorized Privilege Escalation	High	Engage forensics professional to determine extent of compromise. Do not turn off/disconnect system(s) until receiving instructions for forensics professional.	Disclosure may be necessary if a breach has occurred.

DDOS	High	Contact security professional or Internet Service Provider for assistance.	Unnecessary unless client services significantly disrupted or if used in tandem with another attack vector.
Advanced Persistent Threat Identified	High	Engage forensics professional to determine extent of compromise. Do not turn off/disconnect system(s) until receiving instructions for forensics professional.	Disclosure may be necessary if a breach has occurred.

Escalation of Security Events to Management

When a data breach is discovered, the discoverer must obtain sufficient details and notify a member of the incident response team immediately.

At the Branch level, branch personnel must notify Coastal's Incident Response Team of all details immediately. The Team will engage a forensics firm and contact law enforcement as appropriate. The branch incident response team will keep Coastal informed of all material progress, and provide a final report of the resolution of the incident to Coastal for evaluation.

For incidents discovered by Coastal, the incident response team member receiving the report will immediately notify the other team members as well as IT. The firm will report incidents involving a breach to its Cybersecurity insurance carrier and engage a forensics firm if necessary. Management will also contact law enforcement authorities as appropriate.

Incident Identification and Containment

Once a security incident has been identified, the following guidelines will be followed for reporting and containment.

Containment

In the event of a suspected unauthorized access, IT will:

- Determine source of unauthorized access.
- Take appropriate action to control and contain the incident to prevent any further unauthorized access.
- Assist forensics specialists as needed.
- Communicate all actions and updates with the incident response team.

In the event of a suspected data breach, IT will:

- Determine source (external vs internal) and scope of data breach.
- If possible, eliminate source of breached data access.

- Preserve forensic data for analysis.
- Assist forensics specialists as needed.
- Communicate all actions and updates with the incident response team.

In the event of a suspected malware infection, IT will:

- Through the use of an onsite IT technician, remote management systems or user intervention, get infected machine off of the network immediately to prevent any possible spread of the malware infection as well as any potential outbound communications or data transmissions.
- Assist forensics specialists as needed.
- Communicate all actions and updates with the incident response team.

In the event of a reported botnet infection, IT will:

- Through the use of an onsite IT technician, remote management systems or user intervention, get infected machine off of the network immediately to stop further outbound communications with command and control servers.
- Assist forensics specialists as needed.
- Communicate all actions and updates with the incident response team.

In the event of a DDOS or attack on a firm website, IT will…

Contact the web host provider to inform them of the DDOS attack.

- Provide any assistance to hosting company as necessary.
- Communicate all actions and updates with the incident response team.

All responders should follow appropriate escalation procedures and evidence capture procedures for each incident type. Responders can use the following locations to attempt to identify data and records to capture and record network traffic and store packets for post-incident or forensic analysis.

Incident Types	Possible Locations for Relevant Evidence
Network Intrusions	System logs User logs Proxy logs Router & Firewall logs
Email	Mail Servers Router Logs Firewall logs Individual workstations Backup storage Email archive service

Internal Employee/Contractor Activity	System logs Mail Server Logs User Logs Proxy Logs Router & Firewall logs Individual Workstations Electronic organizers Removable Media

For all events and incidents, persons conducting examinations of electronic evidence should be trained and if necessary, certified to conduct the operations performed.

Eradication & Recovery Strategies

Once a security incident has been contained, the following guidelines will be followed for eradication and recovery to restore essential systems to functioning status.

Technical Remediation

- Identify related vulnerabilities
- Identify if the incident is an internal verses external threat
- Eliminate attacker's means of access
- Isolate the network segment of infected workstation(s) prior to taking down any production servers
- Apply upgrades/changes to mitigate vulnerabilities or remove compromised systems from network
- Restore from a known good backup or replace system
- Restore services
- Return system to normal operation
- Perform Risk Assessment ○ Determine what type of data and classification level was exposed ○ Determine compromise, how many records, types, potential losses, etc.

Post Incident Analysis

Post-incident analysis is a reconstruction to establish a clear picture of events that took place during the security incident. It is a valuable opportunity to document lessons learned and identify future best practices, to improve the organization's performance and to provide reference materials for future use. To improve incident response, Coastal will work to accentuate the positive aspects of plans and procedures that functioned correctly and then determine areas of improvement.

Key topics will be:

- *Command and Control*
    - Were current command and control decisions able to be made timely, effectively and efficiently? Does the current executive decision making structure need modifications or enhancements?
- *Operations*
    - What operational changes need to be made to lessen the risks/business impact?

    - How well did staff and management perform in dealing with the incident?
    - Were there performance gaps that could be prevented with pre- planning?
    - Were the documented procedures followed?
    - Were procedures adequate?
    - Were any steps or actions taken that might have inhibited the recovery?
- *Facilities/Resources*
    - What improvements should be made to equipment/facilities/infrastructure to increase the enterprises' security posture to the level of covering unacceptable risks?
    - Are data redundancy and data encryption measures adequate?
- *Support Services*
    - What supplemental support services are needed for more effective response?
    - What, if any, additional human resources are needed?
    - What additional resources need to be implemented to address future incidents? Considerations should include cybersecurity insurance, incident response capabilities, and forensic response capabilities.
    - Were adequate media coverage resources and mandatory reporting capabilities in place?
- *Plans and Procedures*
    - Which plans and procedures need to be created and/or updated to further mitigate risks and enhance communications and reporting guidelines?
- *Training/Equipment Needs*
    - What training is necessary for responders to be prepared for future incidents?
    - What equipment is necessary for responders to be prepared for future incidents?

Review and Testing

This Incident Response Plan is reviewed and updated annually by Mr. Dan Rhoads. The plan is modified to reflect changes in technology, compliance and/or legal requirements.

Finally, in the event of an actual Security Compromise or Security Breach, the plan will be reviewed as part of a post mortem.

A. Incident Response Contact List - Branch

INCIDENT RESPONSE TEAM CONTACT LIST				
Name	**Title**	**Email**	**Office phone**	**Alternate phone**

Keep this updated for your records.

APPENDIX 2
Incident Report Form

Cyber Security Incident Report

Complete the following form when any of the following events has occurred. Include incidents resulting from an accident or negligence, as well as those resulting from deliberate wrongdoing.

1. *Malware was detected on one or more Firm devices.*
2. *Access to a web site or network resource was blocked or impaired by a denial of service attack.*
3. *The availability of a critical web or network resource was impaired by a software or hardware malfunction.*
4. *An unauthorized user breached the network.*
5. *The compromise of a customer's or vendor's computer was used to remotely access the Firm's network resulted in fraudulent activity, such as efforts to fraudulently transfer funds from a customer account or the submission of fraudulent payment requests purportedly on behalf of a vendor.*
6. *The Firm received fraudulent emails, purportedly from customers, seeking to direct transfers of customer funds of securities.*
7. *The Firm was the subject of an extortion attempt by an individual or group threatening to impair access to or damage the Firm's data, devices, network, or web services.*
8. *An employee or other authorized user of the Firm's network engaged in misconduct resulting in the misappropriation of funds, securities, sensitive customer or Firm information or damage to the Firm's network or data.*
9. *The Firm, either directly or as a result of an incident involving a vendor, experienced the theft, loss, unauthorized exposure, or unauthorized use of or access to customer information.*
10. *Any other security breach event.*

Which of the above best describes the incident: (No.#):
*I*f (other) please describe:

Date detected:_____ Date Remediated: _____

How was the incident detected? ☐Internally ☐Externally ☐Not Known

What was the source of the incident? ☐Internal ☐External ☐Not Known Please identify the cause of the incident. ☐Deliberate wrongdoing ☐Error, accident

Was client non-public data compromised? ☐Yes ☐No

Please describe the nature, duration, and consequences of the breach, how it was detected and how it was remediated:

Please provide any additional notes and/or details regarding this event, including the name(s) of any regulatory authorities to which the incident was reported.

Report Submitted by: _____ Date:

Report Reviewed by: _____ Date:

APPENDIX 3 US Law Enforcement Contacts

The US Secret Service Investigative Support Division, centrally located in Washington DC, can assist institutions 24/7 to aid in referring companies to their ECTF's on a 24/7 basis. The USSS-ECTF toll free number is **877-242- 3375**.

Information regarding contacting the USSS-CID or USSS-ECTF can be found at https://www.secretservice.gov/investigation/#field. Contact information for the closest ECTF Office to your office can be found on that web page.

The FBI staffs CY-WATCH for 24/7 incident awareness and response issues. They can be contacted via email **at cywatch@ic.fbi.gov or phone at 855-292-3937**.

Local contact information for USSS is provided here:

ECTF	SUPERVISOR	CONTACT #	MOBILE #	EMAIL
ATLANTA, GA	ATSAIC Marc Debrody	404-331-6111	404-227-3851	marc.debrody@usss.dhs.gov
BALTIMORE, MD	ATSAIC James Meehan	443-263-1000	202-355-3141	james.meehan@usss.dhs.gov
BIRMINGHAM, AL	ATSAIC Nicholas Steen	205-731-1144	205-834-3576	nicholas.steen@usss.dhs.gov
BOSTON, MA	ATSAIC Thomas Baker	617-565-5640	617-990-4152	thomas.baker@usss.dhs.gov
BUFFALO/SYRACUSE, NY	RAIC Timothy Kirk	315-448-0304	315-727-8694	tkirk@usss.dhs.gov
CHARLOTTE, NC	ATSAIC Eric Eversole	704-442-8370	980-207-8809	eric.eversole@usss.dhs.gov
CHICAGO, IL	ATSAIC Troy Land	312-353-5431	312-771-3209	troy.land@usss.dhs.gov
CINCINNATI, OH	RAIC Todd Bagby	513-684-3585	937-684-6204	todd.bagby@usss.dhs.gov
CLEVELAND, OH	ATSAIC Michael Dobeck	216-706-4365	216-973-9272	michael.dobeck@usss.dhs.gov
COLUMBIA, SC	ATSAIC James Ramicone	803-772-4015	803-513-1096	james.ramicone@usss.dhs.gov
DALLAS, TX	ATSAIC Steven Bullitt	972-868-3200	214-784-5996	steven.bullitt@usss.dhs.gov
DENVER, CO	ATSAIC Isaac Barnes	303-850-2700	202-558-8977	ike.barnes@usss.dhs.gov
HONOLULU, HI	ATSAIC Keith Jones	808-462-1404	808-286-1216	keith.jones@usss.dhs.gov
HOUSTON, TX	ATSAIC Marvin Wright	713-868-2299	281-229-4435	mwright@usss.dhs.gov
KANSAS CITY, MO	ATSAIC Jeff Rinehart	816-460-0600	816-500-0351	jeff.rinehart@usss.dhs.gov
LAS VEGAS, NV	ASAIC Gil Lejarde	702-868-3000	702–600-9205	gil.lejarde@usss.dhs.gov
LOS ANGELES, CA	ATSAIC Gregory Auer	213-894-4830	213-598-9353	gregory.auer@usss.dhs.gov
LOUISVILLE, KY	ATSAIC Kirk Mcclelland	502-582-5171	502-263-8906	kirk.mcclelland@usss.dhs.gov
MEMPHIS, TN	ATSAIC James Hawkins	901-544-0333	901-481-2900	jim.hawkins@usss.dhs.gov
MIAMI, FL	ATSAIC Angel Nazario	305-863-5000	305-407-5673	angel.nazario@usss.dhs.gov
MINNEAPOLIS, MN	ATSAIC Mark Johnson	612-348-1800	612-508-9423	mark.johnson@usss.dhs.gov
NASHVILLE, TN	ATSAIC Gregory Mays	615-736-5841	615-788-0150	gregory.mays@usss.dhs.gov
NEWARK, NJ	ATSAIC Russell Wilson	973-971-3100	202-263-9387	russell.wilson@usss.dhs.gov
NEW ORLEANS, LA	SAIC Anthony Bynum	504-841-3260	504-382-3677	anthony.bynum@usss.dhs.gov
NEW YORK, NY	ATSAIC Scott Sarafian	718-840-1000	646-842-1698	scott.sarafian@usss.dhs.gov
OKLAHOMA CITY, OK	ATSAIC David Allison	405-271-0630	405-409-5896	david.allison@usss.dhs.gov
ORLANDO, FL	ATSAIC Keith Hoover	407-648-6333	407-803-3855	keith.hoover@usss.dhs.gov
PHILADELPHIA, PA	SA Ryan Van Deusen	215-861-3300	215-370-1916	ryan.vandeusen@usss.dhs.gov
PHOENIX, AZ	ATSAIC Bradley Keller	602-640-5580	480-220-9099	brad.keller@usss.dhs.gov
PITTSBURGH, PA	ATSAIC Matthew Lavigna	412-281-7825	412-303-2761	matt.lavigna@usss.dhs.gov
SAN FRANCISCO, CA	ATSAIC Kirk Arthur	415-576-1210	415-238-4745	kirk.arthur@usss.dhs.gov
SEATTLE, WA	ASAIC Michael Germain	206-564-5712	202-841-3617	michael.germain@usss.dhs.gov
St. LOUIS, MO	ATSAIC Douglas Roberts	314-539-2238	314-413-9076	douglas.roberts@usss.dhs.gov
WASHINGTON, DC	ATSAIC Chris Gagne	202-406-8000	202-680-8264	christopher.gagne@usss.dhs.gov
LONDON, ENGLAND	SA James Gee	442-07-894-0846	011-447-590-976557	scott.gee@usss.dhs.gov
ROME, ITALY	SA Michael Burgin	390-64-674-2736		michael.burgin@usss.dhs.gov

APPENDIX 4 Password Protection and Construction Guidelines

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or network. All staff, including contractors and vendors with access to Coastal systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Strong passwords are long, the more characters you have the stronger the password. We recommend a minimum of 14 characters in your password. In addition, we highly encourage the use of passphrases, passwords made up of multiple words. Examples include "*It's time for vacation*" or "*block-curious-sunny-leaves*". Passphrases are both easy to remember and type, yet meet the strength requirements. Poor, or weak, passwords have the following characteristics:

- Contain eight characters or less.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Are some version of "Welcome123" "Password123" "Changeme123"

In addition, every work account should have a different, unique password. Whenever possible, also enable the use of multi-factor authentication.

- Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, confidential PII or Coastal information.
- Passwords to Coastal systems must not be inserted into email messages or other forms of electronic communication, nor revealed over the phone to anyone.
- Do not use the "Remember Password" feature of applications (for example, web browsers).

Any user suspecting that his/her password may have been compromised must report the incident to Compliance and change all passwords.

APPENDIX 5

Acceptable Use Policy

Overview

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Coastal. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Coastal employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

These rules are in place to protect the employee and Coastal. Inappropriate use exposes Coastal to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Coastal business or interact with internal networks and business systems, whether owned or leased by Coastal, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Coastal and its affiliates/subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Coastal policies and standards, and local laws and regulation.

This policy applies to employees, contractors, registered persons, access persons, consultants, temporaries, and other workers at Coastal, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Coastal or by a branch using its own equipment to access Coastal systems or information.

The term “Employee” includes all Home Office employees, as well as all independent contractor registered persons, their employees, and associated persons.

Policy

1. General Use and Ownership

i. Coastal proprietary information stored on electronic and computing devices whether owned or leased by Coastal, the employee or a third party, remains the sole property of Coastal. You must ensure through legal or technical means that proprietary information is protected in accordance with Coastal’s Policies and Procedures.

ii. You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Coastal proprietary information.

iii. You may access, use or share Coastal proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

iv. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual branches are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems where these policies are insufficient. In the absence of such policies, employees should be guided by these policies on personal use, and if there is any uncertainty, should consult their supervisor or manager.

v. For security and network maintenance purposes, authorized individuals within Coastal may monitor equipment, systems and network traffic at any time.

vi. Coastal reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2. **Security and Proprietary Information**

i. All mobile and computing devices that connect to the internal network must comply with Coastal's *Cybersecurity Policy*.

ii. System level and user level passwords must comply with the *Password Protection and Construction Guidelines*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited. iii. All computing devices must be secured with a password. You must lock the screen or log off when the device is unattended.

iv. Postings by employees from a Coastal email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Coastal, unless posting is in the course of business duties.

v. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

3. **Unacceptable Use**

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Coastal authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Coastal-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

i. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Coastal.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the

installation of any copyrighted software for which Coastal or the end user does not have an active license is strictly prohibited.

3. Accessing data, a server or an account for any purpose other than conducting Coastal business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a Coastal computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any Coastal account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to Infosec is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network or account.
14. Introducing honeypots, honeynets, or similar technology on the Coastal network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
17. Providing information about, or lists of, Coastal employees to parties outside Coastal.

ii. Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be

addressed to the Compliance Department. The following activity is proscribed when using firm systems or accounts:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Coastal's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Coastal or connected via Coastal's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups, Facebook, Linked In, Twitter or other similar social media. (spam).

iii. Blogging and Social Media

1. Blogging by employees, whether using Coastal's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Coastal's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Coastal's policy, is not detrimental to Coastal's best interests, and does not interfere with an employee's regular work duties. Blogging from Coastal's systems is also subject to monitoring.

2. Coastal's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any confidential or proprietary information when engaged in blogging.

3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Coastal and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Coastal's *Non-Discrimination and Anti-Harassment* policy.

4. Employees may also not attribute personal statements, opinions or beliefs to Coastal when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Coastal. Employees assume any and all risk associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Coastal's trademarks, logos and any other Coastal intellectual property may also not be used in connection with any blogging activity

Policy Compliance

Coastal will verify compliance to this policy through various methods, including but not limited to, archiving reports, internal and external audits, and feedback.

Exceptions

Any exception to the policy must be approved by Compliance in advance. Notwithstanding anything herein to the contrary, as independent contractors, advisors are owners of the client relationships they bring to, and acquire during their tenure, with Coastal.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.