Global Information Security Policy

Introduction

This Global Information Security Policy (the "Policy") forms part of the global information security program adopted by Crawford & Company and its Affiliates (collectively, "Crawford" or the "Company"). The purpose of this Policy is to establish the information security criteria, means, methods, and measures to protect the Company's Information assets and those of our Clients from unauthorized disclosure, modification, or denial through the establishment, implementation, and management of the global information security program.

Policy

Crawford Information Security Program

Crawford shall maintain an information security program designed to protect the confidentiality, integrity and availability of Crawford Information and Information Systems.

Crawford shall designate a qualified individual responsible for overseeing and implementing the Crawford information security program and enforcing the global information security policies. This individual shall report in writing at least annually to the Crawford Board of Directors to report on the Crawford information security program and material cybersecurity risks. The written report shall consider, to the extent applicable:

- The confidentiality of Highly Restricted and Confidential Information and the integrity and security of Crawford Information Systems;
- The global information security policies and procedures;
- Material cybersecurity risks to Crawford Information and Information Systems;
- Overall effectiveness of the Crawford information security program; and
- Material security incidents.

An annual cybersecurity risk assessment must be conducted to identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Information stored on Crawford Information Systems. For more information please refer to the "IT Risk Management Policy".

Crawford has adopted the NIST Cybersecurity Framework (CSF) as the basis for its information security program. The Crawford information security program includes the implementation of global information security policies and procedures to protect Crawford Information and Information Systems from unauthorized access, use and other malicious acts.

Information security policies are intended to provide a common basis for consistent, prudent protection and preservation of the confidentiality, integrity

and availability of Crawford Information Systems. The global information security policies apply to all Crawford entities, locations, and business units and supersede any regional, local or business unit security policies.

Each information security policy will be reviewed and updated by IT management based on a defined schedule requiring, at a minimum, annual review and/or after any significant updates, changes to the environment or security event. Modifications to information security policies shall be reviewed using the same process used for approval of new policies. Information security policies that represent emerging or rapidly changing technologies will be evaluated on a more frequent basis. Each policy is to be evaluated for continued relevance and effectiveness in protecting the Company's Information Systems and to meet regulatory and Client contractual requirements.

Security Awareness and Training

A security awareness program shall be developed, maintained, and managed to ensure Crawford Users receive adequate training and security awareness content. Security awareness techniques can include, for example, displaying posters, generating email advisories/notices, displaying logon screen messages, and conducting information security awareness events.

Mandatory cybersecurity training is provided at least annually for all Crawford employees. The content must include a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents.

Role-based security training shall be provided at least annually to certain Crawford employees with assigned security roles and responsibilities. Simulations or walk-throughs of a cyber-attack shall be periodically conducted to provide training for individuals responsible for identifying and managing Security Incidents.

Information Classification and Handling

All Crawford Users are responsible for ensuring that the proper protection of Crawford Information is maintained. The "Information Classification and Handling Policy" provides the framework for classifying data owned by, managed by and entrusted to Crawford, based on legal requirements, value, criticality and sensitivity, and describes baseline security controls for Crawford Information.

It is imperative for all Crawford Users to comply with the Crawford "Information Classification and Handling Policy" and the "Global Data Protection & Privacy Policy", as well as local laws and regulations regarding data privacy and data protection and with security and privacy clauses in Client contracts, confidentiality

agreements (with Clients, Claimants and other claim parties) entered into with appropriate authority, or court orders.

Incident Reporting

All Crawford Users are required to report all potential Privacy Incidents or Security Incidents immediately upon discovery. All suspected incidents must be reported to Incident_Response@us.crawco.com. In addition to this mandatory reporting, you may also contact the Crawford Help Desk. Once reported, all incident handling processes shall be coordinated by Crawford Global IT Security and/or the Crawford Global Privacy Office. The individual reporting the incident may or may not be informed of the status or results of the investigation, depending on the nature of the incident.

Loss or theft of a Crawford Issued Device must be immediately reported to the Help Desk or by email to Incident_Response@us.crawco.com so that they can initiate the proper response. In addition, a police report must be filed in the jurisdiction where it was stolen.

The specifics of Privacy and Security Incidents should not be discussed widely but should instead be shared on a need-to-know basis. Any communication with external parties will be directed in accordance with Crawford's incident response policies and procedures. For specific information relating to Security Incident response please refer to the "Security Incident Response Policy".

Identity and Access Management

Access to and use of Crawford Information and Crawford Information Systems will be restricted to appropriately identified, validated, and authorized persons on a need-to-know basis.

Prior to being granted access to Crawford Information Systems, the individual shall be screened in accordance with applicable laws. Crawford Human Resources shall define processes for screening individuals and conditions that require rescreening including the frequency of rescreening.

Every Crawford User must have a unique user ID and a password to gain access to the system environment. Passwords must be properly structured, changed, and protected from unauthorized access. Passwords should never be written down by hand or stored electronically by the user.

Regardless of the circumstances, passwords and PINs must never be shared or revealed to anyone other than the authorized user. Similarly, Crawford Users must not perform any activity with user IDs, passwords, or PINs belonging to others.

Crawford Users are responsible for all activity performed with their personal user IDs, passwords, and PINs.

Within one business day, managers must promptly notify Crawford IT when Crawford Users change departments or job duties so that system access rights can be modified to align with the system needs of the new position. Managers must immediately notify Crawford IT when an employee's position has been terminated or a non-employee's duties or contract has been concluded.

For more information, please refer to the "Identity and Access Management Policy".

Internet

The Internet must not be used to communicate, transfer, or store any Highly Restricted or Confidential Information unless the confidentiality and integrity of the information is ensured, the identity of the recipient(s) is established, and the communications are conducted in a secure manner.

Use of externally hosted or cloud-based systems to process or store Highly Restricted or Confidential Information must be reviewed and approved in advance by Crawford Global IT Security. For more information please see the *Third Party Service Providers* section below.

Crawford recognizes that employees might work long hours and occasionally may desire to use the Internet for personal activities at the office or by means of Crawford Issued Devices or Crawford Information Systems. Such use is authorized for a limited time if the usage complies with the law and Company policies at all times and does not incur a detrimental effect on the business performance of the user or any other Crawford User.

Crawford Issued Devices or Crawford Information Systems must not be used to attempt unauthorized entry to a network or the Internet. This includes deliberately releasing malicious software onto the network; engaging in recreational games, obtaining or distributing pornographic, sexually oriented materials; or conducting illegal activity.

Crawford Issued Devices and Information Systems are Company property and subject to monitoring in accordance with local law and applicable Company policies.

To the full extent permitted by applicable laws, Crawford reserves the right to monitor the use of Crawford Information Systems, including anything transmitted through Crawford Information Systems, or via a Crawford Issued Device.

Personally Owned Devices

The use of Personally Owned Devices to store or process Crawford Information is prohibited. Authorized use of Crawford Information Systems that are Internet-based applications (e.g., web-enabled claims systems) for remote access is allowed; however, attachments, files, or other Crawford business content must not be downloaded or saved to a Personally Owned Device.

Email

The Crawford email system must be used predominantly to conduct Crawford business operations. Limited and occasional personal use of the Crawford email system is allowed, provided the content does not have a detrimental effect on the business performance of the user or any other Crawford User.

Sending Crawford Information to a personal email account or any other non-Crawford email account is prohibited. Email messages are to be accessed only by the intended recipient. Crawford Users should check the distribution list and group list prior to sending any emails. Crawford Users should not attempt to gain access to another Crawford User's email account or other computer systems for which they do not have authorized access.

Portable Devices

Crawford Users are responsible for securing portable digital storage media (portable devices) containing Company Information at all times. Portable devices include but are not limited to laptops, notebooks, USB drives, external drives, tablets and smart phones.

Crawford Issued Devices that are portable (e.g., laptops, tablets, smartphones) or physically located outside of a Crawford facility with physical security protections (e.g., desktop at a home or in a common area) must be encrypted.

Crawford Users are prohibited from storing any Crawford Information on any removable storage devices (e.g., USB drive, CD, external hard drive) without approval from Crawford Global IT Security or the Crawford Ethics & Compliance Office. If a removable storage device is approved, Information placed on the removable storage device will be subject to auditable tracking and Information stored thereon must be encrypted.

Crawford Users in the possession of a portable device must physically secure the device when not in use (e.g. secure/locked office or desk, or remain in the person's physical possession).

Information stored on portable Crawford Issued Devices is not included in backup processes. Crawford Users must store Crawford Information from portable Crawford Issued Devices on Crawford servers connected to the Crawford network so the Information is included in backup processes.

Clear Desk and Clear Screen

Crawford Information must not be located or used in areas where an unauthorized person could view Highly Restricted or Confidential information. For more information please see the "Clear Desk Policy".

Third Party Service Providers

Crawford Information and Information Systems must be consistently protected. Third party users with access to Crawford Information and Information Systems must be aware of the limits existing for their use. Access, access rights, and use of Crawford Information and Information Systems by third parties must be limited by the security principles of least privilege, separation of duties, and need-to-know.

Third parties must conduct themselves in a professional manner according to the appropriate roles and responsibilities of their contractual agreements, and in an ethical manner by abiding by, enforcing and ensuring compliance with all information security policies and all related company policies, standards, NDAs, procedures, and documentation.

Any use of a third party service provider to access, process or store Crawford Information shall be reviewed by Crawford Global IT Security and the Crawford Global Privacy Office. The review shall include:

- Identification and risk assessment of the third party service provider;
- Minimum information security practices required to be met by the third party service provider in order for them to do business with Crawford;
- Due diligence process to evaluate the adequacy of security practices of the third party service provider; and
- Periodic assessment of the third party service provider based on the risk they present and the continued adequacy of their information security practices.

If the third party service provider will access, process or store Highly Restricted or Confidential Information, written contractual protections shall address, at a minimum:

- The third party service provider's policies and procedures for access controls to limit access to relevant Information Systems and Highly Restricted or Confidential Information;
- The third party service provider's policies and procedures for use of encryption to protect Highly Restricted and Confidential Information in transit and at rest;
- Notice to be provided to Crawford in the event of a Privacy Incident, Security Incident or event directly impacting Crawford Information Systems or Crawford Information being held or handled by the third party service provider; and
- Representations and warranties addressing the third party service provider's information security policies and procedures that relate to the security of Crawford Information Systems or Highly Restricted or Confidential Information.

For more specific information please refer to the "Global Third Party Risk Management Policy".

Physical Security

Crawford Users must not permit unauthorized persons to pass through doors to restricted areas at the same time as authorized persons. Unknown persons within the secure area should be questioned to ensure they have a legitimate need to be present in the facility. Crawford Users must not prop open doors or disable other physical access control devices.

Physical access to Controlled Areas, such as data centers, server rooms and network closets, where Crawford Information Systems physically reside shall be limited to only those who are formally authorized and possess a business need for access. For more information please refer to the "Physical and Environmental Security Policy".

Definitions

Word or Phrase	Definition
Affiliate	An entity that is owned or controlled by Crawford & Company.
Claimant	The subject of or person filing a claim under a covered Client insurance policy or similar program.

Global Information Security Policy

Word or Phrase	Definition
Client	A current, prior or prospective client of Crawford, and any other party upon whose behalf Crawford acts at the direction of such client.
Confidential Information	Confidential information is highly valuable, sensitive business information and the level of protection is, generally, dictated internally by the Company. Confidential information generally includes all Personal Data, other than business contact information of employees, personnel or vendors, which is not Highly Restricted. See "Information Classification and Handling Policy".
Controlled Areas	Include, but are not limited to, data centers, computer rooms and closets, network control centers and other areas containing Crawford computing equipment, files, data, electrical and telephony circuits and breakers, and environmental controls.
Crawford Information or Information	Means any information received, created, maintained, stored, accessed, held or otherwise processed by or on behalf of Crawford as part of its business operations, including but not limited to research, intellectual property, business and product development plans, sales and marketing business plans, litigation information, information and records about individuals and legal entities with whom we interact or conduct business (e.g., Clients), Claimants, other case parties, suppliers, vendors, contractors, business partners, employees and applicants) and supply chain, finance, human resources, contract, business intelligence and acquisition information. References to Information include any information or data in any format, including audio, visual, written, magnetic, electronic and optical formats. Should additional or revised formats or types of information arise in the future, this Policy will cover any new or revised formats and information types.
Crawford Information Systems	Includes hardware, software, data, networks (landline and wireless), applications, programs, agents, telecommunications equipment, laptops, desktops, mobile devices, communications methods, modes of transmission, tablets, servers, portable, removable or other media, telephones, and other technology, digital devices and systems owned, licensed or managed by or on behalf of Crawford, including , cloud-based and externally hosted applications.
Crawford Issued Device	Laptops, desktops, smart phones, tablets, and removable media purchased and owned by Crawford

Global Information Security Policy

Word or Phrase	Definition
Crawford Users	Includes all full-time employees, part-time employees, temporary employees (including agency staff), agents, consultants and contractors with the ability to view, access and/or process Crawford Information and/or Crawford Information Systems.
Highly Restricted Information	Highly Restricted information is highly valuable, highly sensitive business information and the level of protection for and disclosure of such information is dictated externally by legal and/or contractual requirements. See "Information Classification and Handling Policy".
Personal Data	Means any information relating to an identified or identifiable natural person; it includes Information in any format or media, regardless of whether the information is encrypted. A person may be directly identifiable via their name, address, employee ID, claim number, email address, phone number or government identifier, for example. A person may also be indirectly identifiable through linking or combining additional information that may or may not be in Crawford's custody or control with information in Crawford's custody or control, such as an IP address, MAC address, device identifier, biometric identifier, or other unique identifier, geolocation information, genetic information or DNA, for example.
Personally Owned Devices	Laptops, desktops, smart phones, tablets, and removable media not purchased or owned by Crawford.
Privacy Incident	A Privacy Incident means a violation or threat of violation of privacy laws, principles or Company policies, and includes any event where there is knowledge or reasonable belief that there has been unauthorized or inappropriate collection, use, access, disclosure, transfer, modification, and/or exposure of Personal Data.
Security Incident	A Security Incident is defined as any attempt (successful or unsuccessful) to access and/or adversely affect Crawford internal, client, or claimant data, systems, services or networks in the following context: data confidentiality, integrity, and availability, or illegal access, misuse or escalation of authorized access.

Global Information Security Policy

Scope

This Policy applies to all Crawford Information and all Crawford Information Systems that store, process or transmit Crawford Information. All Crawford Users are required to comply with this Policy. All vendors and third parties with access to Crawford Information should be subject to contractual terms consistent with the requirements of this Policy.

Any exception to this policy must be approved according to the exception process defined in the "IT Risk Management Policy."

Contact

For more information on this Policy, contact the SVP Global IT Security.

Global Information Security Policy

Document Information

Document Name	Global Information Security Policy
Category	Global Information Security Policy
Related Policies	IT Risk Management Policy Information Classification and Handling Policy Global Data Protection & Privacy Policy Security Incident Response Policy Identity and Access Management Policy Acceptable Use Policy Clear Desk Policy Global Third Party Risk Management Policy Physical and Environmental Security Policy
Version No. – Effective Date	Version No. 1.0 - October 31, 2016 Version No. 1.1 – July 24, 2017 Version No. 2.0 – October 19, 2018

Compliance References

Category	Global Information Security Policy
Related Compliance References	HIPAA 164.308(a)(3), ISO/IEC 27001:2013 NIST SP 800-53 Rev. 4 NYDFS 500.07,500.03 SOC2 CC 6.4.1, 6.4.2, 6.4.3 PCI v3.2