Information Classification and Handling Policy

Introduction

This Information Classification and Handling 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 a framework for classifying data owned by, managed by and entrusted to Crawford, based on legal requirements, value, criticality and sensitivity. Classification will aid Crawford in determining the appropriate baseline security and privacy controls for Crawford Information.

Policy

Classification Categories

Crawford Information is categorized into four primary classifications:

- Highly Restricted;
- Confidential;
- Internal Use; or
- Public.

All Crawford Users are expected to apply the classifications and adhere to the controls set forth in this Policy, with respect to any Crawford Information. Asset Owners have primary responsibility for ensuring that Crawford Information and/or Company Information Systems are properly categorized.

The examples set forth in this Policy for each classification level are intended as guidance related to common information types and how they would generally be classified on a risk basis. However, Crawford Users should classify information and Information Systems according to the risk presented in the relevant context. Crawford Users should classify data at a higher classification level than the examples provide if they believe it is warranted by the content and context.

Highly Restricted

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. Highly Restricted data must not be shared with the public, and may not be shared with external parties (e.g., customers, vendors, advisors) without approval of management, and even then unless they have signed a Non-Disclosure Agreement (NDA). Access to internal and external parties must be restricted on a strict need-to-know basis.

Significant damage would occur if Highly Restricted information were to become available to unauthorized internal or external parties, or otherwise be unavailable to Crawford as needed. Such impact could include negatively affecting Company's competitive position, violating legal or regulatory requirements, damaging the

Company's reputation, violating contractual requirements, and posing an identity theft risk.

Examples of Highly Restricted information include:

- Personal Data about Claimants and related parties (e.g., that are a part of claims files maintained for clients), such as name, personal contact details, age, health information, damages, etc.;
- Client reports (e.g., aggregate claims-related information) and information of similar commercial values;
- Client lists;
- Client contract data, billing data, financial account data;
- Communications with external legal counsel, other communications, reports, analyses or documents prepared by or at the direction of legal counsel, or otherwise marked or subject to attorney-client privilege;
- Sensitive Personal Data (employee, Claimant or otherwise), including but not limited to:
    - Personal health information (including Protected Health Information);
    - Payment card data;
    - Biometric data;
    - Social security numbers and other government issued identification numbers;
    - Background and credit checks; and
    - Company account credentials;
- Details regarding ongoing internal investigations;
- Alert Line reports and related investigations;
- Merger and acquisition details;
- Unpublished financial results; and
- Trade Secrets and other proprietary information.

Confidential

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. Confidential data must not be shared with the public, and should not be shared with external parties (e.g., customers, vendors, advisors) unless they have signed a Non-Disclosure Agreement (NDA) or are subject to similar contractual confidentiality obligations. Access by internal and external parties shall be on a need-to-know basis.

Moderate damage would occur if Confidential information were to become available to unauthorized internal or external parties. The impact could include negatively affecting Company's competitive position, damaging the Company's reputation, violating contractual requirements, and exposing the geographic location of individuals.

Examples of Confidential information include:

- Employee Personal Data (e.g., salary, job history, personal contact data) that is not Highly Restricted or business contact data;
- Non-public information about Crawford's products, services, processes, strategies and performance;
- IT network diagrams and configurations;
- Information on facilities and network security;
- Security and privacy incident response records;
- Unpublished market research;
- Privacy impact assessments, third party risk scoring and related questionnaires;
- Internal Company reports;
- Company org charts;
- Intercompany agreements;
- Non-public tax filings, reports, analysis and reviews; and
- Intra-group data sharing or transfer agreements.

Internal Use

Internal Use information may be shared with internal and external parties who have a business need, but may not be released to the general public, due to the negative impact it might have on the Company's business interests. Internal Use data must not be shared with the public, and should not be shared with external parties (e.g., customers, vendors, advisors) unless they have signed a Non-Disclosure Agreement (NDA) or are subject to similar contractual confidentiality obligations.

Minimal or no damage would occur if Internal Use information were to become available to unauthorized internal or external parties. Impact could include damaging the Company's reputation and violating contractual requirements.

Examples of Internal Use information include:

- Business contact information (name, email, phone number, title, company) of employees, personnel, vendors, suppliers, clients and business partners;
- Client contracts, and related documents and contractual terms;

- Meetings notes;
- Internal corporate policies;
- Internal operating procedures and operational manuals; and
- Marketing and promotional campaign development and related materials.

Public

Public information is information that has been approved for release to the general public and is freely sharable both internally and externally, via open communication sources such as print media or the Internet.

No damage would occur if Public information were to become available to internal or external parties. The impact of such release would not be damaging or a risk to business operations.

Examples of Public information include:

- Marketing brochures and leaflets;
- Product and service brochures;
- Public-facing webpages;
- Job opening announcements;
- News releases; and
- Financial statements and other reports generally publicly available.

Information Protection and Handling

This section provides guidance on how to handle Crawford Information and the physical security requirements and secure transmission of Crawford Information internally and externally to ensure that all Crawford Information is properly handled within the organization or by an approved external third party. These guidelines are based on globally accepted data protection practices for implementing proper controls for collecting, processing, storing and disposing of data.

Crawford Users are responsible for safeguarding Crawford Information against unauthorized disclosure, modification, and destruction and in accordance with the guidelines defined in this Section.

Data Inventory

An inventory of all systems and network devices in the Highly Restricted and Confidential data environment must be made and updated when a significant change occurs in the system environment. A review of this inventory must be completed at least semi-annually or when a change has occurred.

Data network and flow diagrams, identifying where Highly Restricted and Confidential data is stored, processed, or transmitted must be documented. Data network and flow diagrams must be reviewed at least semi-annually or when a change has occurred.

Data Access and Review

Access to data will be based on business need and the need-to-know. Any third party wishing to access Crawford Information classified as anything other than Public must sign a Non-Disclosure Agreement (NDA) prior to be giving access. Third parties must, at minimum, ensure the data protection controls in this document are implemented prior to being given access to Crawford Information. Reviews of audits trails documenting access and disclosure of information must be reviewed at minimum on a semi-annual basis.

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

Data Capture

A risk analysis must be conducted to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of data held by the Company prior to any collection or processing.

Key parts of the analysis include, but are not limited to:

- Identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles;
- Assessing the criticality of those information assets; and
- Identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events and identifying the vulnerabilities of the identified assets.

Data in Transit

In the event that data is transmitted to a recipient outside the Company network to a third party this party must agree to maintain a data protection level equivalent to this Policy. This does not apply if transmission is based on a legal obligation.

All data being transferred between systems, including Crawford Information sent over the Internet, through email or other means (e.g., automated reports), must be protected according to its classification. Data classified as Highly Restricted or Confidential must be encrypted when being transferred. Data classified as Internal

or Public need not be encrypted during transmission unless otherwise specified by the originator of the data.

When sending Highly Restricted or Confidential Information over email, Crawford Users must exercise care to ensure that the recipient's email address(es) is correct, that the content of the message, including any attachments, is intended for all recipients, and that they comply with established protection mechanisms when sending Highly Restricted or Confidential Information through email.

When sending hard copy reports or communications containing Highly Restricted or Confidential Information, care must be taken to ensure that distribution is limited to individuals and companies that are intended to receive the Information. Care must be taken to ensure that only the correct information is sent to the intended recipient.

Any third parties accessing Highly Restricted or Confidential data should always enable encryption during transport and at rest.

Reproduction of Highly Restricted or Confidential data will be kept to the absolute minimum as required to conduct business operation. The data will be disposed of in the manner as required in the Data Disposal section of this Policy.

The use of Personally Owned Devices to store Highly Restricted or Confidential Information is prohibited.

Data at Rest

Highly Restricted or Confidential data will be encrypted at rest. Data classified as Internal Use or Public need not be encrypted as rest unless otherwise requested by the originator of the data.

Crawford Users needing to store data on a non-standard system or application, or outside of the Company systems, will need to work with the Crawford Security team for an acceptable solution for data encryption.

A data discovery tool will be implemented to validate Highly Restricted or Confidential data at rest. These scans must be conducted against systems that store, process, and transmit data to verify no inadvertent storage of Highly Restricted or Confidential data.

Highly Restricted and Confidential data being stored on removable media, mobile devices or approved portable storage devices must be encrypted at rest.

Papers containing Highly Restricted or Confidential Information must be physically secured (e.g., in a locked file cabinet or desk) when not in use.

The use of Personally Owned Devices to store Highly Restricted or Confidential Information is prohibited.

Data Disposal

Disposal of data should be performed when the data is no longer necessary for legal, regulatory, or business reasons and in accordance with the "Records and Information Management Policy." Crawford Information Systems should be configured to automatically remove stored Highly Restricted or Confidential data on a periodic basis in accordance with the "Records and Information Management Policy."

Printers, Copiers and Fax Machines

Printers, copiers and fax machines that are used to process Highly Restricted or Confidential Information must be placed in secure locations and areas not easily accessible to unauthorized persons. If equipment cannot be relocated to a secure location, a sign will be posted near the equipment indicating that unauthorized persons are prohibited from viewing documents from the equipment.

When printing Highly Restricted or Confidential Information, the Crawford User must be present at the printer at the time that printing is output to prevent the information from being revealed to unauthorized parties, or direct the output to a printer inside an area where only authorized employees are permitted.

All documents containing Highly Restricted or Confidential Information must be promptly removed from the printer, copier or fax machine and placed in an appropriate and secure location.

If a printer, copier, or fax machine jams or malfunctions when printing Highly Restricted or Confidential Information, the involved users must not leave the machine until all copies of the Highly Restricted or Confidential Information are removed or are no longer legible.

The repair of fax machines, printers, and copy machines must be performed only by third-party vendors who have signed a Non-disclosure Agreement (NDA).

Definitions

Information Classification and Handling Policy

Word or Phrase	Definition
Affiliate	An entity that is owned or controlled by Crawford & Company.
Asset Owner	The person or entity that has been delegated formal responsibility for the security of an asset, asset category, or data hosted on the asset. Asset Owners are responsible for making sure that assets are secure while they are being developed, produced, maintained and used.
Claimant	The subject of or person filing a claim under a covered Client insurance policy or similar program.
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".
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.

Information Classification and Handling Policy

Word or Phrase	Definition
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
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.

Word or Phrase	Definition
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.

Scope

This Policy applies to all Crawford Information and all Crawford Information Systems that store, process or transmit Crawford Information. All Crawford Information and Crawford Information Systems should be categorized according to the classification levels set out in this Policy. 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.

Information Classification and Handling Policy

Document Information

Document Name	Information Classification and Handling
Category	Global Information Security Policy
Related Policies	Identity and Access Management Policy Records & Information Management Policy IT Risk Management Policy
Version No. – Effective Date	Version 1.0 – October 31, 2016 Version 2.0 – October 19, 2018

Compliance References

Category	Data Protection
Related Compliance References	GDPR - Article 30, ·Article 24, HIPAA Security Rule 45 C.F.R. 164.308(a)(1)(ii)(A), 164.308(a)(3)(ii)(A), 164.308(a)(8), 164.310(d), 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.310(b), 164.310(c), 164.312(a), 164.312(e) 164.310(d)(2)(i), 164.310(d)(2)(ii)), 164.312(a)(1), 64.312(a)(2)(iii), 164.312(a)(2)(iv), 164.312(b), 164.312(c), 164.308(a)(7)(ii)(E), 164.308(a)(1)(ii)(D), 164.308(b)(1), 164.310(d164.314(b)(2)(i), 164.312(d) PCI DSS v3.2 - 1.1.3, Req 3.1, 9.8 PCI DSSv3.5, 3.7, 4.1 PCI DSS v4.2, 4.3 SOC2 3.2.6, 6.1.5, 6.5.1, 7.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8, SC-1, SC-8, 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4, DM-2, MP-6 ISO/IEC 27001:2013 A.10.1.1 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7,A.10.1.1 NYDFS 500