

Records and Information Management Policy

Introduction

Crawford & Company (“Crawford” or the “Company”) recognizes that while information is crucial to its business and can have great value, it also can pose great risk if not managed properly. The governance of Company information assets, therefore, requires an enterprise strategy and framework to enable the Company to make decisions about information for the benefit of the organization, beyond any individual department or function.

It is the Company’s policy to use and maintain information in accordance with all applicable laws and regulations in the jurisdictions in which it operates, as well as governing operating requirements and contractual agreements. The Records and Information Management Policy (“Policy”) has been developed to ensure that the Company retains Records which it has a legal, regulatory, contractual or business need to retain, as well as routinely disposing of information in the normal course of business under the approved Records Retention Schedule.

Policy

Policy Objectives

The goal of this Policy, which is integral to Crawford’s Information Governance strategy, (“IG”), is to develop a coordinated strategy for managing the Company’s Records and information resources, which is intended to satisfy relevant compliance requirements, manage information risks, and support efforts by Crawford to optimize the value of its data assets. Additionally, this Policy seeks to enable an open but secure environment for collaboration and information sharing, both internally and with the Company’s network of Third Parties and customers.

Specific objectives include:

- Demonstrating compliance with applicable laws and regulations
- Managing retention of Record in compliance with applicable client contractual obligations upon us
- Coordinating information identification and classification
- Optimizing the efficiency and management of storage
- Decreasing unnecessary storage volumes by disposing of redundant, outdated, and trivial (ROT) content
- Reducing costs and risks associated with eDiscovery, regulatory compliance, data privacy, and information security
- Preserving and protecting the privacy and confidentiality of Records that contain Personal Data or confidential information relating to clients,

Records and Information Management Policy

customers, employees, and Third Parties in accordance with applicable privacy laws and regulations, contractual obligations, and other Crawford policies

- Identifying and preserving Records and information that are essential to the continuity of Company business operations, or necessary to identify its assets, obligations, or liabilities, including in the event of a natural or man-made disaster or other incident
- Facilitating the identification, preservation, and accurate production of Records relevant to any legal or regulatory process, threatened or actual litigation, or investigation involving Crawford
- Increasing collaboration and secure information sharing among Crawford employees, Third Parties, clients and customers
- Providing for the periodic review of Policy compliance to ensure the currency, practicality, and performance of the Policy

This Policy supports a comprehensive Information Governance framework, leveraging, coordinating, and reconciling Records Retention, disposition, Legal Hold, and broader Records and Information Management and eDiscovery-related requirements with other information focused disciplines and initiatives within the Company, including those relating to information security, data privacy, information asset classification, business continuity, and data governance.

The Company also requires the lifecycle of documentation necessary for the conduct of business and the accessibility of Records and information content to be definite and controlled. To this end, this Policy specifically addresses the retention and destruction of all Records and Non-Record Content, regardless of media or format, which are created or received pursuant to the conduct of business related to the Company, its employees, clients, customers and Third Parties in accordance with the Records Retention Schedule.

Records

“Record” means documented information, whether paper or electronic, that is generated, created or received by directors, officers, employees or other parties acting on behalf of Crawford, which is valuable to, or necessary for, Crawford’s operations. Company Records may be in multiple forms, mediums of transmission or recording. For example, Company Records include, but are not limited to reports, letters, memoranda, e-mail, facsimiles, graphics, data, audits, expense reports, meeting minutes, handwritten notes, calendars, agenda, outlines, timelines, summaries, presentations, statistical analyses, research materials, charts, photographs, bound record books, publications, manuscripts, drawings, cards, maps and audio and video media and recordings. Company Records do not include library books, periodicals, stock copies of reports, blank forms or stationery.

Records and Information Management Policy

Company Records are necessary to satisfy the needs of everyday business operations, legal and regulatory requirements, fiscal responsibilities and historical needs. Records serve as documentary evidence of an organization, business transaction, decision, operation, policy, procedure, formal communication, analysis or event.

These Records are key resources and essential assets that are critical to conducting Company business since they may:

- Provide evidence of the Company's business transactions
- Document the Company's policies and procedures
- Allow the Company to refer to past documentation to make informed business decisions
- Provide Company staff with the information necessary to respond quickly and effectively to customers
- Demonstrate that the Company acted in accordance with its own policies and in adherence with the law in the conduct of business
- Support the Company's actions and business decisions in the event of litigation, audit, or government investigation

Records (Active/Inactive)

Active Records are those that may be referenced frequently or at intervals for legitimate business purposes and should remain with the business or designated vendor authorized to house Company active Records. Inactive Records are those no longer required for carrying out the functions for which they were created and should be archived and disposed of in accordance with the Records Retention Schedule

Records Ownership

Company Records do not belong to individual employees or Third Parties. Employees who have Crawford Records in their custody must return those Records to the Company upon request or when leaving employment. Third Parties must be required to return Company Records upon request.

Records Retention

Crawford must maintain certain types of Records for specified periods of time pursuant to business, legal, regulatory, and contractual requirements. The Records Retention Schedule is the Company's standard for retention and disposition of all Company Records. If new business functions and operations are developed at Crawford, the Records Retention Schedule will be updated to include Records associated with the new functions and operations as necessary. Employees shall notify the Legal Department of additional Record types that may

Records and Information Management Policy

need to be included in the Records Retention Schedule including those known to be held by Third Parties.

In general, Crawford maintains client Records pursuant to its contractual obligations to clients. Crawford may establish default retention periods by jurisdiction (the “Default Period”) for client Records. Where Crawford is contractually required to retain client Records, it may do so by reference to these established default retention periods, unless the agreement between Crawford and the client requires a different retention period. Under the relevant Records Retention Schedule, the applicable retention period for client Records should be set forth as the “Default Period, unless otherwise established by client’s instructions.”

Records shall be retained and disposed of in a systematic manner, in accordance with the Company’s approved Records Retention Schedule. All exceptions to or exemptions from the Records Retention Schedule must be approved by the Legal Department.

Records Destruction / Disposition

Records shall be disposed of at the end of the retention period defined by the Records Retention Schedule, unless destruction is suspended in accordance with a Legal Hold, or an exception or exemption is approved by the Legal Department. To ensure complete disposal and protect against unauthorized disclosure of the contents of the Records, all Records should be destroyed in a secure manner through an approved vendor for hard copy or electronic Records.

Legal Hold

On occasion, the periods found in the Records Retention Schedule could come into conflict with a legal or regulatory obligation. In such instances, the need to comply with the relevant legal or regulatory obligation will temporarily override the Records Retention Schedule. The Legal Department is responsible for issuing a Legal Hold notice to suspend Records from destruction, and shall have decision-making authority for the identification, preservation and safekeeping of Records that are subject to a Legal Hold. Once the Legal Department removes the Legal Hold, which will be clearly communicated by them in writing, the normal retention and destruction periods will resume in accordance with the Records Retention Schedule.

Employees will cooperate with a Legal Hold order and no attempt should be made by any employee to alter or destroy Records subject to a pending or reasonably anticipated legal or regulatory investigation as this could damage the Company’s ability to deal with the investigation effectively and could lead to criminal prosecution of the employee.

Protection and Access to Records

Records and Information Management Policy

All Records shall be maintained in an organized manner to ensure that they can be located and used when needed. Records shall remain readable, retrievable, and accessible throughout the applicable retention period. Records shall be protected in safe and secure conditions commensurate with the sensitivity of information in accordance with the Crawford Information Classification and Handling Policy.

Employees and Third Parties who create and retain Records containing Personal Data must ensure that such information is secured against unauthorized access. This includes taking steps in accordance with Crawford's Information Security Policy and Data Protection and Privacy Policy to ensure that only authorized individuals are granted access to such content, as well as utilizing secure disposal methods to destroy or dispose of Records that contain confidential or proprietary Information.

Responsibilities for Records

See also the Global Information Classification & Handling Policy

Managers

Managers oversee the implementation, coordination and facilitation of Records and information management activities, standards, and procedures for Record management within their organization. Their responsibilities include:

- Facilitating and monitoring compliance of employees with this Policy and associated procedures and processes
- Ensuring Records are secured and transitioned when employees leave the Company, including compliance with all retention and preservation requirements
- Ensuring the integrity, accessibility, authenticity, reliability, quality, and usability of official Company Records are maintained when system decommissions, modifications, and data migrations occur and when developing new systems, applications, workflows, and/or Record repositories
- Coordinating with Third Parties who have Records in their possession, requiring them to securely retain and return or destroy any such Records in accordance with this Policy

Custodians and/or System Administrators

Custodians and/or System Administrators are responsible for:

- Safeguarding protected information
- Determining appropriate levels of Information Classification and access controls based on the Information Classification and Handling Policy

Records and Information Management Policy

- Noting exceptions for Legal Hold /Notice of Non-Destruction
- Ensuring appropriate storage, handling, distribution, use, and destruction of Records
- Reporting compliance violations

Employees

All employees are responsible for implementing, coordinating, and facilitating Records and information management activities, standards, and procedures. Specifically, employees are individually responsible and accountable for compliance with:

- Retaining Records in accordance with the Records Retention Schedule
- Protecting Company Records from unauthorized or improper access, use, or disclosure
- Complying with this Policy and associated procedures and processes

Crawford employees are responsible for ensuring that Third Parties handling Company Records and information retain the content in accordance with this Policy and the terms of the Third Parties' contract.

Definitions

Custodians

Company employees and Third Parties entrusted with the custody and safekeeping of Company Records or information resources.

Discovery / eDiscovery

The process of identifying, preserving, collecting, analyzing, reviewing, and producing hard copy and Electronically Stored Information (ESI) for the purposes of proving or disproving facts, theories, or allegations to resolve disputes or to respond to government or investigatory inquiries.

Electronically Stored Information (ESI)

Electronic Records and Imaged Records, as well as any electronically stored Non-Record Content that is potentially responsive to a legal eDiscovery request.

Information Governance (IG)

Information Governance is a strategic, coordinated, and interdisciplinary approach that seeks to satisfy information compliance requirements, manage information risks, and optimize information value.

Non-Record Content

Records and Information Management Policy

Non-Record Content is any form of information, material, or data that is recorded or preserved incidentally or without intent to create a Record, including reference or unofficial copies, and which do not need to be retained to satisfy Company Records Retention Schedule requirements.

Personal Data is defined in the Global Privacy and Data Protection Policy, and includes any information that identifies, could be used to identify, or is linkable to an individual person, including information that is inaccurate or out of date. For example, it includes: name, business or personal contact details, identification number, education and work history; background checks, credit checks, and criminal records history; salary, benefits, and financial details; performance reviews; accident and incident reports and claims data; location data, IP address and online identifier; one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity, or other personal characteristics; and medical conditions or health information, and family status.

Records Retention Schedule

The Records Retention Schedule is the standard for retention and disposition of Company Records, including functional Record categories with a unique code, description, and retention requirement that incorporates legal, operational, and business requirements for retention.

Systems of Record

Designated electronic repositories within which original, official and imaged Records are maintained for retention purposes.

Systems Administrators

Designated IT Managers responsible for systems administrative decisions directly affecting the retention, purge, and destruction of referenced or stored Records in the systems.

Third Party

Any entity or person, other than a client, that is not under the direct business control of Crawford with whom Crawford engages in a business relationship, including any vendor, supplier, support provider, fulfilment provider, agent, consultant, advisor, contractor, business, marketing or strategic partner, joint venture, associate and correspondent. See the Global Third Party Risk Management Policy for more detail.

Scope

This Policy applies to the Company and its subsidiaries, covering all employees entrusted with the custody or governance of Company information, regardless of media or format, including its creation, classification, storage, access, sharing,

Records and Information Management Policy

dissemination, protection, and disposition. The content of this Policy that applies to Third Parties entrusted with Records will be addressed in contracts with them and reflected in the Third Party Risk Management Policy.

Failure to comply with this Policy may result in disciplinary action up to and including termination.

Contact

For more information on this Policy, contact the General Counsel or the Global Ethics & Compliance Office.

Document

Information

Document Name	Records and Information Management Policy
Category	Global Policy
Related Policies	<ul style="list-style-type: none"> ▪ Crawford Code of Business Conduct and Ethics ▪ Information Security Policy ▪ Information Classification and Handling Policy ▪ Third Party Risk Management Policy ▪ Data Protection and Privacy Policy
Version No. – Effective Date	<ul style="list-style-type: none"> ▪ Version No. 1.0 (Global Records & Information Management Policy) – November 1, 2014 ▪ Version No. 2.0 - March 28, 2018