



## Global Data Protection and Privacy Policy

### Introduction

Crawford & Company and its majority-owned and controlled subsidiaries (collectively “Crawford” or “the Company”) have adopted this Global Data Protection and Privacy Policy (“Policy”). Crawford recognizes the importance of privacy and security, and is committed to complying with applicable Data Protection Laws and Client contractual requirements in handling Personal Data.

### Purpose

Although Data Protection Laws vary by jurisdiction, all Crawford Personnel should be aware that laws exist to protect the privacy and security of Personal Data, and these laws impact the manner in which Crawford and its Personnel use, access, disclose, or otherwise Process such information.

This Global Data Protection and Privacy Policy (“Policy”):

- sets forth the principles that apply to the Processing of Personal Data by Crawford, and describes how Crawford adheres to these principles; and
- provides an overview of Crawford’s privacy governance structure, and the roles and responsibilities of key individuals and groups in carrying out Crawford’s privacy compliance obligations and tasks.

This Policy will be supplemented by additional policies, procedures and guidelines, to address specific areas, jurisdictions, laws and requirements.

### Scope

This Policy applies to all Personal Data that is Processed by Crawford as a Data Controller or a Data Processor, including relating to its Personnel, Clients, Claimants, Vendors and other parties. All Personnel are required to adhere to this Policy. Personnel that violate this Policy may be subject to disciplinary action, subject to applicable local law and employment terms.

All Personnel have an important role to play in the proper management and safeguarding of Personal Data, in identifying data protection and data handling issues as they arise, and in escalating them immediately to the Global Privacy Office. All Personnel are also expected to cooperate as necessary in implementing the principles, requirements and key components of this Policy.

---

### Principles

- 1. Fair, Transparent and Lawful Processing.** Personal Data will be collected, stored and Processed fairly, lawfully and in a transparent manner. This means:
  - 1.1. Individuals will be informed of the Processing (by the Data Controller).



## Global Data Protection and Privacy Policy

- 1.2. Personal Data is Processed in accordance with the stated purposes for its collection or similar compatible purposes, and subject to a lawful legal basis such as consent where required by law.
- 1.3. Personal Data is not processed in ways that the Data Subject would not reasonably expect.
- 1.4. When acting as a Data Processor, Personal Data will only be Processed as necessary for performing the services as directed by Clients, or where otherwise required by applicable law.
- 2. Data Minimization.** Personal Data will be collected only where reasonable and necessary for the stated purposes for which it is being Processed, and will be adequate, relevant and limited to what is necessary in relation to those purposes.
- 3. Purpose Limitation.** Personal Data will be Processed for specified, explicit and legitimate purposes, and in a manner compatible with the purpose for which the Personal Data was initially collected.
- 4. Accuracy.** Personal Data will be accurate and up-to-date.
  - 4.1. Reasonable steps will be taken to ensure the accuracy of Personal Data obtained.
  - 4.2. Inaccurate Personal Data (considering the purposes of its Processing) will be erased or rectified.
- 5. Limited Retention.** Personal Data will be retained only for as long as is necessary to achieve the specified purpose(s), subject to applicable Data Protection Laws and Client contractual requirements.
- 6. Security and Integrity.** Appropriate organizational, administrative and technical security measures will be in place to safeguard the Personal Data, provide for secure Processing of Personal Data, and identify, prevent, detect and mitigate risks to Personal Data and the systems, tools and processes used to Process Personal Data.
  - 6.1. Personal Data will be Processed in a manner that provides for appropriate security of the Personal Data.
  - 6.2. Security measures must be designed and implemented to safeguard against unauthorized and unlawful Processing, and accidental loss, destruction or damage of Personal Data and related systems.
  - 6.3. Controls will be designed and implemented to detect, mitigate and remediate security events and incidents.
  - 6.4. Policies and procedures will be established so that event, security incidents and privacy incidents are promptly reported internally, and investigated, assessed and handled in accordance with the

## Global Data Protection and Privacy Policy

established Data Protection Laws where they may impact Personal Data or related Processing activities.

**7. Privacy by Design.** Activities and processes will be designed, implemented and carried out in a way that provides at the outset for compliance with the above principles and the integration of necessary safeguards for Personal Data.

**8. Accountability.**

Compliance with these principles will be assessed, and Processing activities will be conducted in a manner that demonstrates compliance, and can be audited and assessed.

8.1. Inquiries and complaints related to Personal Data Processing will be assessed, responded to and resolved (where possible) fairly and without undue delay.

8.2. Reasonable processes for receiving, handling and responding to questions, requests and complaints from individuals and Clients are established, to provide for fair, timely, consistent and lawful responses.

8.3. Accurate records of Processing activities will be maintained, including records of security incidents, complaints, Data Subject requests and other mandatory records under applicable Data Protection Laws.

---

### Key Privacy Compliance Components

In order to comply with the principles set forth above, Crawford must take steps to ensure that these principles are addressed within all relevant business processes and activities, and to implement certain processes and procedures, which includes the following key components, each of which is addressed below in this Policy:

- Notice to Individuals
- Legal Basis of Processing
- Recordkeeping (and Records of Processing)
- Data Subject Rights
- Third Party and Vendor Management
- Incident Response
- Privacy Awareness and Training
- Privacy Impact Assessments
- Ongoing Assessments and Audits



## Global Data Protection and Privacy Policy

- Governance
- 

### Notice to Individuals

Crawford will notify Data Subjects of the Personal Data that it Processes about them as required by Data Protection Law, including notice of the following: the types of Personal Data collected, the purposes of the Processing, Processing methods, the Data Subjects' rights with respect to their Personal Data, the retention period, potential international data transfers, if data will be shared with third parties and the Company's security measures to protect Personal Data.

For employees, this information will be set forth in an employee privacy notice and additional notices, as required under applicable Data Protection Law. Where applicable, employee privacy notices will be provided to new employees during onboarding, and a copy of the privacy notice will also be posted online where possible, and available through local human resources contacts. Employees will be notified and provided a copy of applicable employee privacy notices whenever material changes are made.

For Clients, Vendors and other relevant third parties, a privacy notice should be provided or made available in a retrievable and an easily accessible manner, where practicable at the point of the collection of Personal Data or as soon thereafter as is reasonable.

---

### Legal Basis of Processing

Personal Data may only be collected and Processed by Crawford in compliance with applicable Data Protection Laws, and where required with the consent of the Data Subject. When acting as a Data Processor, Personal Data will only be Processed as necessary for performing the services as directed by Clients, or where otherwise required by applicable law.

Whenever Personal Data Processing is based on the Data Subject's explicit consent, a record of such consent must be made and maintained.

Personal Data that is subject to EU Data Protection Laws may only be Processed pursuant to specific lawful basis under the law. Where Crawford is the Data Controller, it is responsible for ensuring that the Processing is conducted pursuant to one or more specific legal bases (e.g., consent, necessary to perform contract with individual, legitimate business purpose, required by law, necessary to defend rights) and that the legal basis has been disclosed to Data Subjects in the relevant privacy notice.

---



## Global Data Protection and Privacy Policy

**Recordkeeping** Crawford will maintain accurate records of its Processing activities, including mandatory records as set forth in applicable Data Protection Laws. The Global Privacy Office maintains a data inventory/record of processing of Crawford's Processing of Personal Data as required under EU Data Protection Laws. The EU Group Data Protection Officer is responsible for ensuring that the record of processing is updated as appropriate.

---

**Data Subject Rights** Data Subjects have specific rights related to their Personal Data and how it is Processed. Data Subjects will be provided with a reasonable mechanism to enable them to access their Personal Data, to exercise any other applicable rights, such as the right to update, rectify, erase or transmit in portable form their Personal Data, if appropriate or required by law ("Data Subject Rights"), and to inquire or submit a complaint related to the Processing of their Personal Data.

### Data Processor

When acting as a Data Processor, Crawford will, in accordance with applicable laws and contractual requirements, notify the Data Controller of any Data Subject requests to exercise their Data Subject Rights and provide reasonable support upon request to enable the Data Controller to respond to the request as required by Data Protection Laws.

### Data Controller

When acting as a Data Controller, Crawford is responsible for respecting Data Subject Rights and responding to related requests as required by Data Protection Laws. The Chief Privacy Officer or a delegate will provide guidelines for responding to such requests; all Personnel are responsible to following such guidelines.

**Cross-border transfers of Personal Data** Applicable Data Protection Laws and Client commitments may require Crawford to take steps to protect Personal Data before it transfers the Personal Data out of the country from which it is collected.

### Equivalent Protection.

Crawford must take steps to ensure that cross-border transfers of Personal Data are subject to adequate safeguards. Personal Data that is transferred cross-border must be Processed by or on behalf of Crawford in accordance with applicable Data Protection Laws, and Client commitments.

### Restricted Transfers

Restricted Transfers of Personal Data must be carried out in accordance with applicable Data Protection Laws and Client commitments.



## Global Data Protection and Privacy Policy

In order to properly Process such Personal Data, Crawford has adopted various measures, to ensure that Personal Data is adequately protected when transferred outside the jurisdiction from which it was collected.

Where there is any Restricted Transfer of Personal Data, adequate safeguards must be used, including the execution of the Standard Contractual Clauses where relevant. Crawford will assess whether any authorization from relevant Supervisory Authorities or Clients is necessary.

### Transfers Amongst Crawford Group

Crawford has executed an Intra Group Data Processing Agreement, which incorporates the Standard Contractual Clauses, in order to provide adequate safeguards for Restricted Transfers amongst Crawford group entities, as well as other Processing of Personal Data by one or more Crawford group entity on behalf of one or more other Crawford group entity.

Each Crawford group entity will sign onto the Intra Group Data Transfer Agreement, and comply with the Intra Group Data Transfer Agreement with respect to any transfers or Processing amongst Crawford group entities. As new entities become part of Crawford, each new entity will be required to sign onto the Intra Group Data Transfer Agreement.

### Transfers to Vendors

Before any Restricted Transfer to a Vendor occurs, Crawford will take steps to incorporate the Standard Contractual Clauses into the applicable contractual agreement between Crawford and the Vendor.

---

### **Third Party and Vendor Management**

Business relationships with and engagement of third parties must be conducted in a manner that complies with this Policy and applicable Data Protection Laws and Client commitments.

Vendors and Subprocessors may only be engaged if they are capable of meeting adequate standards and providing appropriate safeguards for Personal Data.

#### At a minimum:

- Appropriate due diligence should be conducted of all Vendors and Subprocessors, prior to their Processing of Personal Data (including storage or access), and on an ongoing basis thereafter as needed (subject to the Crawford third party risk management program).
- Appropriate contractual obligations must be implemented with each Vendor, which include (where relevant) contractual obligations that are equivalent to those which apply to Crawford under its relevant Client contracts.

## Global Data Protection and Privacy Policy

- Crawford must take steps to incorporate the Standard Contractual Clauses into the applicable contractual agreement between Crawford and the Vendor, if there may be any Restricted Transfer.
- All necessary steps under applicable Data Protection Laws and Client contractual commitments will be completed.

Vendors and other third parties must be assessed, engaged and managed in accordance with the Crawford third party risk management program.

---

### **Incident Response**

Adequate controls are necessary so that security incidents that may impact Personal Data are detected, reported, and handled in accordance the established policies and procedures, including the Global Incident Response Policy, and applicable Data Protection Laws.

When a security event or a security incident may impact Personal Data or indicate a violation of this Policy, Data Protection Laws or Client commitments, the Global Privacy Office must be promptly notified.

The Global Privacy Office is responsible for assessing, investigating and determining the response and notification obligations arising out of a privacy event or privacy incident, and all Personnel are required to cooperate with the Privacy Office as necessary to assess, investigate, mitigate, report and resolve privacy events and incidents. The Global Privacy Office has the sole authority to determine if a privacy event or incident is a Data Breach; Personnel should not speculate or identify any incidents as Data Breaches unless directed to by the Global Privacy Office.

Where a Data Breach is determined, Crawford must act promptly to provide any required notice to relevant Clients, Supervisory Authorities and Data Subjects.

---

### **Privacy Training and Awareness**

Privacy governance and data protection are critically important to Crawford, and its ability to:

- Comply with laws and Client contractual commitments
- Control risks
- Maintain trust
- Operate effectively
- Support strategic goals and data governance model

## **Global Data Protection and Privacy Policy**

### Annual Training

Mandatory privacy and security training will be required for all Personnel at least annually regarding privacy, data protection and information security.

### Additional Role-based Training

Personnel with roles that involve regular handling of Personal Data and those with specific key responsibilities within the privacy governance structure will receive additional role-based training and resources, as appropriate.

### Embedded Privacy Resources

Privacy liaisons will be identified across the company to support privacy initiatives, raise awareness amongst colleagues and liaise with the Global Privacy Office.

### **Privacy Impact Assessments**

It is critically important that activities and processes are designed, implemented and carried out in a way that provides for compliance with Data Protection Laws and Crawford policies and the integration of necessary safeguards for Personal Data. This is a key component of the privacy by design principle (see Principle 7 above).

Crawford has developed a policy and procedures for conducting privacy impact assessments, and where necessary, formal data protection impact assessments.

### Privacy Impact Assessments

Privacy Impact Assessments (PIA) must be conducted to assess the privacy impact of and identify risks related to projects, activities and Vendors that may impact the privacy and security of Personal Data. Prior to engaging a new Vendor, starting a new project, designing or materially updating a new system, combining data from two systems or record sets, or otherwise engaging in any new or substantially changed activity or process that may impact Personal Data or how it is Processed, a PIA must be conducted.

### Data Protection Impact Assessments

Where a PIA indicates that the Processing of Personal Data is likely to result in a high risk to individuals' rights and freedoms, a formal data protection impact assessment (DPIA) will be conducted prior to such Processing, in order to determine the nature of those risks and mitigate such risks to the extent possible. Such Processing may not begin until the Privacy Advisory Committee has determined that the risks from the Processing have been adequately mitigated.



## Global Data Protection and Privacy Policy

### Ongoing Assessment and Updates

Ongoing risk assessments will be conducted of relevant business processes and systems will be conducted to:

- verify that internal controls, policies and procedures are in place and being followed; and
- identify any compliance gaps.

Privacy compliance processes and procedures will be updated to account for:

- new threats or risks to the business that have been identified;
- changes to operations and activities;
- changes in privacy laws; and
- areas for improvement based on risk assessments results, PIA, audits, complaints, lessons learned from incident response efforts, and/or other means.

### Governance

#### Global Privacy Office

Crawford has established a Global Privacy Office, which is designed to develop, manage and drive enterprise-wide privacy initiatives. At a high level, the Global Privacy Office:

- Initiates and fosters a culture of privacy within Crawford
- Ensures that privacy is included in business objectives and goals
- Manages compliance in a complex regulatory environment

The Global Privacy Office carries out the above with input from and collaboration with various functions within Crawford, such as Legal, Ethics & Compliance Office, Information Technology and Information Security.

#### Chief Privacy Officer

The Chief Privacy Officer leads the Global Privacy Office and has overall responsibility and accountability for privacy within Crawford. This includes:

- Developing and maintaining this Policy and supporting policies and procedures;
- Setting the direction and priorities for Crawford's privacy compliance program, including implementation of enterprise-wide privacy objectives; and
- Management of budget and resources (including Data Protection Officers).



## Global Data Protection and Privacy Policy

Global service lines, departments and local entities are accountable for initiation and implementation of the enterprise-wide privacy objectives in consultation with the Chief Privacy Officer.

### **Data Protection Officers and Data Privacy Officers**

Crawford has created additional roles with formal responsibility for compliance with Data Protection Laws in specific regions and jurisdictions, as set forth below. Crawford will appoint individuals to these roles. These individuals are accountable to the Chief Privacy Officer regarding their relevant duties to oversee compliance with this Policy, related data protection policies and procedures and applicable Data Protection Laws.

#### European Union

The Data Protection Officer is a statutory role required by EU Data Protection Laws under certain conditions. Crawford will establish one or more Data Protection Officer roles within the EU, with responsibility for EU Data Protection Laws in a particular jurisdiction or on behalf of the Crawford group.

- Group Data Protection Officer. The EU Group Data Protection Officer has responsibility for monitoring and advising on Crawford's compliance with EU Data Protection Laws, as well as assisting with the regular update of the mandatory records of Processing, and providing input on mandatory DPIA. An EU Group Data Protection Officer will be a member of the Global Privacy Office, and report to the Chief Privacy Officer, but must be able to exercise his/her duties independently. The EU Group Data Protection Officer will be supported by local Privacy Leads in the relevant EU jurisdictions.
- Country Data Protection Officer. A country-specific EU Data Protection Officer may be internally or externally appointed, and will have responsibility for data protection compliance in a particular jurisdiction and report to the Country Manager for that jurisdiction.

Each EU Data Protection Officer that is appointed will be subject to terms that guarantee his/her independence and impartiality. The Data Protection Officer's role is not commercial, and the Data Protection Officer must not be put in a situation (e.g., through the assignment of additional responsibilities) that might create a conflict of interest. Each EU Data Protection Officer will have independence to carry out his/her statutory duties, and to report on matters related to compliance with EU Data Protection Laws to the highest levels of management as follows:

- The EU Group Data Protection Officer is able to communicate matters related to compliance with EU Data Protection Laws to the Global Executive Management team.



## Global Data Protection and Privacy Policy

- A country-specific EU Data Protection Officer is able to communicate matters related to compliance with Data Protection Laws in a particular jurisdiction to the Country Manager for that jurisdiction.

An up-to-date record of the current EU Data Protection Officer appointees will be maintained by the Privacy Office, and must also be disclosed in relevant Data Subject privacy notices, and notified to the relevant Supervisory Authorities as required by applicable EU Data Protection Laws.

### The Philippines

A Philippine Data Protection Officer is required for each Crawford Philippine entity. A Philippine Data Protection Officer may be appointed for one or more Philippine entities, and will have responsibility for overseeing compliance with Philippine Data Protection Laws and submitting any registrations required under applicable Data Protection Laws to the Philippine National Privacy Commission. A Compliance Officer for each Philippine entity may be appointed to support the Philippine Data Protection Officer. The current Data Protection Officer for each Philippine entity will be notified to the Philippine National Privacy Commission.

### Canada

The Canadian Data Privacy Officer will be appointed for one or more Canadian entities as required under Canadian Data Protection Laws, and will have responsibility for overseeing compliance with Canadian Data Protection Laws.

### Other Jurisdictions

Where required by applicable Data Protection Laws, Crawford will designate additional roles with formal responsibility for privacy and data protection in particular jurisdictions, who will be accountable to the Chief Privacy Officer regarding their relevant duties to oversee privacy compliance.

### **EU Privacy Leads**

A Privacy Lead will be appointed for each Crawford EU entity, to support the EU Group Data Protection Officer in receiving, reviewing and responding to inquiries and complaints from Client, Data Subjects and Supervisory Authorities, and conducting any necessary DPIA.

### **Privacy Coordinators**

Unless an exception is granted by the Global Privacy Office, each Affiliate and each global department will assign a Privacy Coordinator who is responsible for being a shared point of contact between the Global Privacy Office and its entity or department, and for identifying on-the-ground compliance issues and escalating these to the Global Privacy Office, and assisting the Global Privacy Office in implementing privacy initiatives. The Privacy Coordinators



## Global Data Protection and Privacy Policy

are accountable to the Chief Privacy Officer regarding their relevant responsibilities.

An EU Privacy Lead may also serve as a Privacy Coordinator.

### Privacy Advisory Committee

The Privacy Advisory Committee is a senior, cross-functional group established to discuss data protection compliance and management issues that warrant a cross-functional examination or decision. The Privacy Advisory Committee is led by the Chief Privacy Officer, and membership includes all internal Data Protection Officers and Data Privacy Officers, as well as representatives from key departments, including the Ethics & Compliance Office, Legal, Information Technology and Information Security.

The Committee meets at least quarterly, and reports to the Global Executive Management team. The Committee will prepare an annual report to be presented to the Crawford Board of Directors, or designated committee, summarizing significant events during the previous calendar year (e.g., milestones achieved).

The Privacy Advisory Committee is expressly permitted to raise with the Global Executive Management team, and where appropriate the Crawford Board of Directors (or designated committee), on an ad-hoc basis, issues or comments related to potentially high-risk projects or possible instances of material non-compliance.

---

### Definitions

**“Client”** means a current, prior or prospective client of Crawford, and any other party upon whose behalf Crawford acts at the direction of such client.

**“Client Personal Data”** means Personal Data that Crawford Processes (as a Data Processor) on behalf of its Clients.

**“Data Controller”** or **“Controller”** means the natural or legal person/entity that alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

**“Data Processor”** or **“Processor”** means the natural or legal person/entity that Processes Personal Data on behalf of the Controller.

**“Data Protection Laws”** means, to the extent applicable to Crawford, the laws, rules and regulations regarding privacy and data protection or otherwise governing the Processing of Personal Data (including EU Data Protection Laws).

**“Data Subject”** means the individual to whom the Personal Data relates.

**“EEA”** means the European Economic Area.

## Global Data Protection and Privacy Policy

**“EU Data Protection Laws”** means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the EU General Data Protection Regulation 2016/679 (“GDPR”) and laws implementing or supplementing the GDPR, as well as any successor UK data protection legislation to the GDPR adopted if the United Kingdom exits the European Union.

**“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 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.

**“Data Breach”** means any known or reasonably suspected unauthorized access to, use, disclosure or other Processing of Personal Data, as well as any loss, theft or acquisition of Personal Data, or any incident that compromises the security of Personal Data.

**“Personnel”** means all full-time, part-time, temporary, regular and contract employees, consultants and non-employee workers.

**“Process”** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of the data.

**“Restricted Transfer”** means a transfer of Personal Data by, among, or to Crawford (including any Crawford group entities) across national borders that is prohibited by applicable Data Protection Laws or Client agreements, in the absence of the Standard Contractual Clauses.

**“Sensitive Data”** means Personal Data that is considered sensitive or otherwise subject to heightened regulatory standards under Data Protection Laws (including “special categories of Personal Data” under EU Data Protection Laws), and Personal Data that, if accessed or disclosed without authorization, could lead to identity theft or material financial, physical or reputational harm, as well as including: race or ethnicity; religious or philosophical beliefs; trade union membership; political affiliation; sexual orientation or private life; health information, medical treatment; disability information; Protected Health Information; mental health; genetics;



## Global Data Protection and Privacy Policy

biometrics; credit card or financial account number; Payment Card Data; Social Security number or government identifiers; credit report or background checks; and criminal history or proceedings.

**“Standard Contractual Clauses”** means:

- (a) for Personal Data subject to EU Data Protection Laws, the EU standard contractual clauses for the transfer of Personal Data to Processors located in third countries, or any successor thereto or alternative data transfer mechanism, recognized by the European Commission pursuant to the GDPR (Articles 44-46); and/or
- (b) for Personal Data subject to Data Protection Laws other than EU Data Protection Laws, other national equivalents established to ensure adequate protection for cross-border transfers of Personal Data.

**“Subprocessor”** means a Vendor appointed by or on behalf of a Crawford entity (in their capacity as a Data Processor) which will Process Client Personal Data.

**“Supervisory Authority”** means the relevant regulatory authority with regard to Data Protection Laws, including the supervisory authority as defined under EU Data Protection Laws.

**“Vendor”** means a third party Data Processor (including a Subprocessor) that provides goods or services to a Crawford entity or to another entity or person on behalf of a Crawford entity.

---

### Contact

The owner of this Policy is the Chief Privacy Officer. For more information, contact the Global Privacy Office ([privacy@global.crawco.com](mailto:privacy@global.crawco.com)).

---



## Global Data Protection and Privacy Policy

### Document Information

<b>Document Name</b>	Global Data Protection and Privacy Policy
<b>Category</b>	Global Policy
<b>Related Policies and Documents</b>	Personal Data Management Policy Third Party Risk Management Policy Global Incident Response Policy Records & Information Management Policy Code of Business Conduct and Ethics
<b>Approved by</b>	Elizabeth Alaniz, Chief Privacy Officer
<b>Version No. – Effective Date</b>	1.0 - May 2018