Global Information Security Policy

Revised: 09-21-2015

1. Policy

Information Security refers to the processes and methodologies that are designed and implemented to protect print, electronic, or any other form of confidential information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption. Crawford & Company's ("Crawford's") business operations are critically dependent on information and Information Systems, and Crawford is entrusted with collecting and handling confidential, private and sensitive information about Crawford's operations and personal information about individuals including employees, clients (i.e., the party that engages Crawford and pays for or facilitates the payment of Crawford's fees), claimants and business partners (e.g., third-party vendors, contractors).

Crawford is responsible for protecting the confidentiality, integrity and availability of confidential, private and sensitive information, regardless of medium. Crawford's policy is to comply with all applicable data protection and privacy laws in the countries in which Crawford conducts business. As such, compliance with Crawford's information security and privacy controls is mandatory, and all Crawford staff must be aware of, understand, and comply with any security-related standards, policies, procedures, and practices that pertain to their activities and areas of responsibility, including:

- Global Information Security Policy
- Information Classification and Handling Policy
- Email Acceptable Use Policy
- Global Data Protection and Privacy Policy
- Global Records and Information Management Policy
- Social Media and Internet Acceptable Use Policy

The Crawford Global Information Security Policy is available from Crawford management and stored in the Policies & Procedures section on the Crawford Intranet at www.accesscrawford.com. Local country polices and/or procedures may articulate requirements regarding information security and the above-listed topics, but the Global Information Security Policy takes precedence.

Exceptions to this policy must be reviewed and approved by the applicable regional Security Exceptions process.

2. Scope and Definitions

The Crawford Global IS Policy applies to all (non-Garden City Group) Crawford Users, confidential information, and Crawford Information Systems. These terms and certain other terms used in this document are defined as follows:

Crawford Users – includes all full-time employees, part-time employees, temporary employees, consultants and contractors with the ability to view, access and/or process confidential information and/or Crawford Information Systems.

Confidential Information – is information which, if disclosed to unauthorized parties, could have serious impact on Crawford's interests including competitiveness and business growth; the ability to comply with laws and regulations; and the integrity and public trust of the Crawford name. Examples include employee information (e.g., salary, benefits, personal contact information), client information (e.g., contract information, billing information, credit limits), claimant information, other claim party information, business partner information, and information about Crawford's products, services, processes, strategies and performance. See the Information Classification and Handling Policy for further guidance.

Crawford Information Systems – includes hardware, software, data, networks (land and wireless), telecommunications, laptops, desktops, mobile devices, tablets, removable media, telephones, recorded conversations, and data housed in systems managed by Crawford and/or third parties, cloud-based applications, and externally hosted applications.

Crawford-Issued Devices – laptops, desktops, smartphones, tablets purchased and owned by Crawford.

Personally Owned Devices – laptops, desktops, smartphones, tablets not purchased or owned by Crawford.

3. Implementation

3.1 *Global Information Security and Privacy Office*

In order to ensure that appropriate information security is applied throughout the organization, Crawford has established a cross-functional Global Information Security and Privacy Office, responsible for the planning, implementation, and administration of Crawford's Information Security and Privacy initiatives, including the creation of policies, processes, tools, and controls designed to protect confidential, private and sensitive information.

Crawford's Executive Management has designated the Global Chief Information Officer ("CIO") as the chair of the Global Information Security and Privacy Office. The Global CIO provides regular updates on information security topics and initiatives to Crawford Executive Management and the Board of Directors.

3.2 *Information Classification and Handling*

Crawford Users are responsible for ensuring that the proper protection of confidential information is maintained throughout its lifecycle. It is imperative for all Crawford Users to comply with Crawford's Information Classification and Handling Policy, as well as local legislation regarding data privacy and data protection and with security and privacy clauses in client contracts and confidentiality agreements (with claimants and other claim parties) entered into with appropriate authority.

For more information on information classification and handling guidelines, please refer to the Information Classification and Handling Policy.

3.3 *Access to Confidential Information*

Access to and use of confidential information and Crawford Information Systems will be restricted to appropriately identified, validated, and authorized persons on a need-to-know basis. Managers are responsible for authorizing and approving requests to access Crawford's information and Information Systems. Consideration will be given to establish Crawford User access capabilities based on authorized business requirements.

Managers are also responsible for ensuring that Crawford User access rights are periodically reviewed and removed when no longer required, either through suspension, termination of employment, or changes in assigned responsibilities.

Management approval is required before a user is authorized to use any Crawford Information Systems or access any confidential information (including hard copy information and files). The approval must be documented and retained for audit purposes.

Managers shall ensure that Crawford Users are positively and individually identified and authenticated before giving access to view, process, update, modify, and/or delete confidential information or Crawford information systems.

3.4 *Acceptable Use of Crawford-Issued Devices and Crawford Information Systems*

Crawford-issued devices are provided for conducting company business and accessing employment-related information. Crawford-issued devices or Crawford Information Systems must not be used to attempt unauthorized entry to a network via 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.

Any unattended active workstation, laptop, smartphone, tablet or device capable of holding or transferring confidential information must be secured from unauthorized access and must not be left unprotected.

The use of personally owned devices (e.g., home computer, tablet, or smartphone) to store or process confidential information is prohibited. Authorized use of Internet-based applications (e.g., web-enabled claims systems) for remote access is allowed; however, attachments or files must not be downloaded or saved to a Personally Owned Device.

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 as long as the usage complies with the law and company policies at all times.

Since Crawford-issued devices and Information Systems are company property, there is no expectation of privacy. This includes browsing history, email, social media posts or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on Crawford Information Systems.

Crawford reserves the right to monitor the use of Crawford Information Systems, including anything transmitted through Crawford's electronic communication systems, or via a Crawford-issued device.

3.5 *Email Acceptable Use*

The Crawford email system should be used predominantly to conduct Crawford's 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.

The Crawford email system and all contents of the emails are the property of Crawford. Crawford reserves the right, to the extent permissible under the applicable law, to monitor employee use of its systems, including Crawford email and personal email accounts accessed from Crawford-issued devices. All messages composed, sent or received through the Crawford email system become the property of Crawford and are stored in the email system and/or on backup copies.

Email messages are to be treated as confidential and accessed only by the intended recipient. 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. Any requests to access email accounts of existing or former Crawford Users must be approved in writing by the lead Human Resources or Risk & Compliance Group individual for the applicable region/business unit/location.

Email Users must conduct themselves in a professional manner when composing and sending email communications and refrain from sending email communications that could be viewed as obscene or that might constitute harassment or bullying. Examples of such behavior might include offensive posts that could contribute to a hostile work environment on the basis of race, gender, disability, religion or other status protected by law or common policy.

Email communications sent or received using Crawford's email system must not be used for advertisements, solicitations, or chain letters; soliciting or promoting political or religious causes; gambling, pornography, or violent purposes; or any unlawful activity.

The email system shall not be used to send (upload) or receive (download) copyrighted materials, software, trade secrets, proprietary financial information, or similar materials without appropriate authorization.

Email distribution lists in the system are the property of Crawford regardless of the originator of such lists. As such, email distribution lists cannot be released to anyone outside Crawford without the prior approval of the Vice President of Corporate Communications.

Email Users are required to change their passwords regularly and as prompted by the email system. Passwords are to be kept confidential and not revealed. Passwords can be shared with an authorized ICT technician to facilitate troubleshooting, maintenance, or installation of hardware or software. In such instances, the password must be changed immediately after the completion of the work.

Email Users must not cause or permit the transmission of Crawford business-related content, whether confidential information or not, to the User's personal or home email accounts or to any other party who does not have a legitimate business need for the information or is otherwise authorized by Legal or Risk & Compliance Group to do so.

Confidential Information sent over the Internet through email or other means must be secured and protected while in transit. Many clients contractually require encryption or other secured transmissions (e.g., password-protected zip file) when sending claimant information through 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 Confidential information through email.

3.6 *Social Media and Internet Acceptable Use*

Internet and Intranet systems are provided for use in conducting Crawford business and accessing employment-related information.

The Internet should not be used to communicate, transfer, or store any 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 Crawford confidential information must be reviewed and approved by the Information Security and Privacy Office.

Crawford Users must comply with copyright laws and applicable licensing requirements. Downloading of non-Crawford executable software and copyrighted materials using the Internet is prohibited for security and legal reasons.

3.7 *Records & Information Management*

Paper, film, tapes, CDs, and other removable media containing confidential information must be shredded or destroyed prior to discarding.

Confidential information in hard-copy form should be properly marked, and the number of copies and people to whom sensitive information is distributed shall be controlled.

Confidential information must not be removed from Crawford premises except when in relation to Crawford business. When removed from Crawford premises, such information must be appropriately safeguarded.

Crawford Users must backup and store confidential information on non-portable devices (i.e., Crawford servers connected to Crawford's network). Portable storage devices should not be connected to Crawford computers, systems or networks without a specific authorized business purpose. If a portable device is used, encryption of confidential information on the portable device is mandatory. All portable devices storing information should be under the direct physical control of the individual using such devices at all times.

Hard copy confidential information must be physically secured when left in the office outside of business hours. Confidential information should not be left unattended on a desk, table, or elsewhere. Confidential information should be erased from whiteboards, flip charts, or similar common locations.

3.8 *Password Requirements*

Crawford Users with the authority to add, maintain and remove Users within any system or application ("System Administrators") that processes and/or stores Confidential Information, are responsible for ensuring such system or application password requirements align with Crawford's Password Policy. Passwords must be properly structured, changed, and protected from unauthorized access.

Passwords unique to an individual must not be shared with other individuals or other Crawford Users. Temporary or initial passwords may be shared with the User's supervisor, but only to facilitate password delivery to Users that cannot receive them using approved delivery methods. If a password must be shared with a User's supervisor or an authorized ICT technician to facilitate troubleshooting, maintenance, or installation of hardware or software, then the User must change the password immediately after the completion of the work.

Any use of the username and password by anyone other than the person to whom the user name and password are properly issued is prohibited.

3.9 *Conduct Not Prohibited by this Policy*

This policy is not intended to preclude or dissuade employees from engaging in activities protected by state or federal/national law, including the U.S. National Labor Relations Act or any equivalent in other countries, such as discussing wages, benefits or other terms and conditions of employment, forming, joining or supporting labor unions, bargaining collectively through representatives of their choosing, raising complaints about working conditions for their own and their fellow employees' mutual aid or protection or legally required activities.

3.10 *Privacy and Security Incident Reporting*

Managers are responsible for overseeing Crawford User activities and reporting any potential security incidents or violations. Disciplinary matters resulting from violations of Information Security policies are handled by local managers under the direction of individuals from ICT, Human Resources, Legal and/or any applicable risk and compliance function, as necessary.

A Privacy Incident is an 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 Confidential information about an individual, such as, protected health information ("PHI"), personally identifiable information ("PII"), or debit/credit cardholder data.

A Security Incident occurs when there is any attempt to access or adversely affect data, systems, or networks that affects their confidentiality, integrity, or availability, and may or may not involve exposure of PHI, PII and/or debit/credit cardholder information.

All Privacy and Security Incidents must be reported in one of three ways:

a) Report the incident directly to your ICT Service Desk (United States and EMEA/AP), or through an online notification through the ESAM procedure (Canada);
b) Send an email to Incident_Response@us.crawco.com
c) Report the incident to your supervisor or manager. Supervisors or managers must then escalate the report using the channels described above.

The global incident reporting procedure should be followed whenever:

a) Confidential information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties;

b) Unauthorized use of confidential information or information systems has occurred or suspected of occurring or when passwords or other system access control mechanisms are lost, stolen, or disclosed;

c) There is any unusual system behavior, such as missing files, frequent system crashes, misrouted messages, or similar behavior, which may indicate a computer malware infection.

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 by Legal, any applicable risk and compliance function, and/or a member of the Global Executive Management team.

Policy Name	Global Information Security Policy
Policy Number	Global_IS Policy 00001
Effective Date	09-21-2015
Approved By	Brian Flynn
Last Approval Date	09-21-2015

Intellectual Property