Política Global de Segurança da Informação

Documento

Índice

Introdução

Esta Política Global de Segurança da Informação (a "Política") faz parte do programa global de segurança da informação adotado pela Crawford & Company e suas Afiliadas (coletivamente, "Crawford" ou a "Empresa"). O objetivo desta Política é estabelecer os critérios, meios, métodos e medidas de segurança da informação para proteger os ativos de informação da Empresa e os de nossos clientes contra divulgação, modificação ou negação não autorizada por meio do estabelecimento, implementação e gerenciamento do programa global de segurança

da informação.

Âmbito

Esta Política se aplica a todas as Informações da Crawford e a todos os Sistemas de Informação da Crawford que armazenam, processam ou transmitem Informações da Crawford. Todos os usuários da Crawford são obrigados a cumprir esta Política. Todos os fornecedores e terceiros com acesso às Informações da Crawford devem estar sujeitos a termos contratuais consistentes com os requisitos desta Política. Qualquer exceção a esta política deve ser aprovada de acordo com o processo de exceção definido na "Política de Gerenciamento de Riscos de Segurança Cibernética". O não cumprimento desta Política pode resultar em ação disciplinar que pode incluir rescisão.

Definições

Afiliada significa uma entidade que pertence ou é controlada pela Crawford & Company.

Proprietário do Ativo significa a pessoa ou entidade a quem foi delegada a responsabilidade formal pela segurança de um ativo, categoria de ativo ou dados hospedados no ativo. Os proprietários de ativos são responsáveis por garantir que os ativos estejam seguros enquanto estão sendo desenvolvidos, produzidos, mantidos e usados.

Reclamante significa o sujeito ou a pessoa que registra uma reclamação sob uma apólice de seguro coberta do Cliente ou programa semelhante.

Cliente significa um cliente atual, anterior ou potencial da Crawford, e qualquer outra parte em cujo nome a Crawford atue sob a direção de tal cliente.

As Informações Confidenciais são informações comerciais confidenciais e altamente valiosas e o nível de proteção é, geralmente, ditado internamente pela Empresa. As informações confidenciais geralmente incluem todos os Dados Pessoais, exceto informações de contato comercial de funcionários ou fornecedores, que não são confidenciais. Consulte "Política de Classificação e Tratamento de Informações".

As Áreas Controladas incluem, mas não estão limitadas a, data centers, salas de informática e armários, centros de controle de rede e outras áreas contendo equipamentos de computação Crawford, arquivos, dados, circuitos e disjuntores elétricos e telefônicos e controles ambientais.

Informações ou Informações da Crawford significa qualquer informação recebida, criada, mantida, armazenada, acessada ou processada por ou em nome da Crawford como parte de suas operações comerciais, incluindo, mas não se limitando a pesquisa, propriedade intelectual, planos de desenvolvimento de negócios e produtos, planos de negócios de vendas e marketing, informações sobre litígios, informações e registros sobre pessoas físicas e

jurídicas com as quais interagimos ou conduzimos negócios (por exemplo, Clientes), Requerentes, outras partes do caso, fornecedores, vendedores, contratados, parceiros de negócios, funcionários e candidatos) e cadeia de suprimentos, finanças, recursos humanos, contrato, inteligência de negócios e informações de aquisição.

As referências a informações incluem quaisquer informações ou dados em qualquer formato, incluindo formatos de áudio, visual, escrito, magnético, eletrônico e óptico. Caso surjam formatos ou tipos de informações adicionais ou revisados no futuro, esta Política cobrirá quaisquer formatos e tipos de informações novos ou revisados.

A Crawford Information Systems inclui hardware, software, dados, redes (fixas e sem fio), aplicativos, programas, agentes, equipamentos de telecomunicações, laptops, desktops, dispositivos móveis, métodos de comunicação, modos de transmissão, tablets, servidores, mídias portáteis, removíveis ou outras mídias, telefones e outras tecnologias, dispositivos e sistemas digitais de propriedade, licenciados ou gerenciados por ou em nome da Crawford, incluindo aplicativos baseados em nuvem e hospedados externamente.

Dispositivos emitidos pela Crawford significa laptops, desktops, smartphones, tablets e mídias removíveis adquiridos e de propriedade da Crawford.

Os usuários da Crawford incluem todos os funcionários em tempo integral, funcionários em meio período, funcionários temporários (incluindo funcionários de agências), agentes, consultores e contratados com a capacidade de visualizar, acessar e/ou processar as Informações da Crawford e/ou os Sistemas de Informação da Crawford.

Incidente de segurança é definido como qualquer tentativa (bem-sucedida ou malsucedida) de acessar e/ou afetar adversamente dados, sistemas, serviços ou redes internas, de clientes ou reclamantes da Crawford no seguinte contexto: confidencialidade, integridade e disponibilidade de dados ou acesso ilegal, uso indevido ou escalonamento de acesso autorizado.

Informações confidenciais são informações comerciais altamente valiosas e confidenciais e o nível de proteção e divulgação de tais informações é ditado externamente por requisitos legais e/ou contratuais. Consulte "Política de Classificação e Tratamento de Informações".

Dados Pessoais significa qualquer informação relacionada a uma pessoa física identificada ou identificável; inclui Informações em qualquer formato ou mídia, independentemente de as informações serem criptografadas. Uma pessoa pode ser diretamente identificável por meio de seu nome, endereço, ID de funcionário, número de reivindicação, endereço de e-mail, número de telefone ou identificador do governo, por exemplo. Uma pessoa também pode ser indiretamente identificável por meio da vinculação ou combinação de informações adicionais que podem ou não estar sob custódia ou controle da Crawford com informações sob custódia ou controle da Crawford, como endereço IP, endereço MAC, identificador de dispositivo, identificador biométrico ou outro

identificador exclusivo, informações de geolocalização, informações genéticas ou DNA, por exemplo.

Dispositivos de propriedade pessoal significa laptops, desktops, smartphones, tablets e mídias removíveis não comprados ou de propriedade da Crawford.

Incidente de Privacidade significa uma violação ou ameaça de violação das leis, princípios ou políticas da Empresa de privacidade e inclui qualquer evento em que haja conhecimento ou crença razoável de que houve coleta, uso, acesso, divulgação, transferência, modificação e/ou exposição não autorizada ou inadequada de Dados Pessoais.

Incidente de segurança é definido como qualquer tentativa (bem-sucedida ou malsucedida) de acessar e/ou afetar adversamente dados, sistemas, serviços ou redes internas, de clientes ou reclamantes da Crawford no seguinte contexto: confidencialidade, integridade e disponibilidade de dados ou acesso ilegal, uso indevido ou escalonamento de acesso autorizado.

Política

Programa de segurança cibernética de Crawford

A Crawford deve manter um programa de segurança cibernética baseado em risco e projetado para proteger a confidencialidade, integridade e disponibilidade da Crawford Information and Information Systems. A Crawford designará um Chief Information Security (CISO) que será responsável por supervisionar e implementar o programa de segurança cibernética e fazer cumprir as políticas globais de segurança da informação. O CISO deve relatar por escrito pelo menos anualmente ao Conselho de Administração da Crawford sobre o programa de segurança cibernética da Crawford, incluindo, na medida aplicável:

- A confidencialidade das Informações da Crawford e a integridade e segurança dos Sistemas de Informação da Crawford.
- Políticas e procedimentos globais de segurança da informação.
- Riscos materiais de segurança cibernética para a Crawford Information and Information Systems.
- Eficácia geral do programa de segurança da informação de Crawford.
- Eventos significativos de segurança cibernética e mudanças no programa de segurança cibernética.
- Planos para remediar inadequações materiais.

A gerência executiva sênior deve supervisionar o programa de segurança cibernética, inclusive recebendo e revisando regularmente relatórios gerenciais sobre questões de segurança cibernética, ameaças relevantes à segurança cibernética e a eficácia do programa de segurança cibernética, e confirmando que recursos suficientes

são alocados para implementar e manter um programa de segurança cibernética eficaz.

Uma avaliação de risco de segurança cibernética deve ser realizada anualmente para identificar e avaliar os riscos de segurança cibernética internos e externos que possam ameaçar a segurança ou a integridade das informações armazenadas nos Sistemas de Informação da Crawford. Para obter mais informações, consulte a "Política de Gerenciamento de Riscos de Segurança Cibernética". Os resultados da avaliação são revisados e usados para informar o design do programa de segurança cibernética.

O programa de segurança cibernética da Crawford inclui a implementação de políticas e procedimentos globais de segurança da informação documentados para proteger a Crawford Information and Information Systems contra acesso não autorizado, uso e outros atos maliciosos. As políticas de segurança da informação destinam-se a fornecer uma base comum para proteção e preservação consistentes e prudentes da confidencialidade, integridade e disponibilidade da Crawford Information and Information Systems. As políticas globais de segurança da informação se aplicam a todas as entidades, locais e unidades de negócios da Crawford e substituem quaisquer políticas de segurança regionais, locais ou de unidade de negócios. Cada política de segurança da informação deve ser revisada, atualizada e aprovada pela gerência de TI anualmente e após quaisquer atualizações ou alterações significativas no ambiente dos sistemas de informação. Cada política deve ser avaliada quanto à relevância e eficácia contínuas na proteção das Informações e Sistemas de Informação da Empresa e para atender aos requisitos regulamentares e contratuais do Cliente.

Conscientização e treinamento em segurança cibernética

Um Programa de Conscientização sobre Segurança Cibernética deve ser desenvolvido, mantido e gerenciado para garantir que os Usuários da Crawford recebam treinamento adequado e conteúdo de conscientização sobre segurança. Para obter mais detalhes, consulte a "Política de Conscientização e Treinamento em Segurança Cibernética" de Crawford. O treinamento obrigatório de segurança cibernética deve ser fornecido pelo menos anualmente para todos os funcionários da Crawford. O conteúdo deve incluir uma compreensão básica da necessidade de segurança da informação e ações do usuário para manter a segurança e responder a suspeitas de incidentes de segurança. O treinamento de segurança baseado em funções deve ser fornecido aos funcionários da Crawford com funções e responsabilidades de segurança específicas. Simulações ou orientações de um ataque cibernético devem ser realizadas periodicamente para fornecer treinamento para indivíduos responsáveis pela identificação e gerenciamento de Incidentes de Segurança.

Classificação e tratamento de informações

Todos os usuários da Crawford são responsáveis por garantir que a proteção adequada das informações da

Crawford seja mantida. A "Política de Classificação e Tratamento de Informações" fornece a estrutura para classificar os dados de propriedade, gerenciados e confiados à Crawford, com base em requisitos legais, valor, criticidade e sensibilidade, e descreve os controles de segurança de linha de base para a Crawford Information. É imperativo que todos os Usuários da Crawford cumpram a "Política de Classificação e Tratamento de Informações" e a "Política de Proteção de Dados e Governança de Informações", bem como as leis e regulamentos locais relativos à privacidade e proteção de dados e com cláusulas de segurança e privacidade em contratos de Clientes, acordos de confidencialidade (com Clientes, Reclamantes e outras partes reivindicadoras) celebrados com a autoridade apropriada, ou ordens judiciais.

Relatório de incidentes

Todos os usuários da Crawford são obrigados a relatar todos os possíveis incidentes de privacidade ou incidentes de segurança imediatamente após a descoberta para Incident_Response@us.crawco.com. Uma vez relatados, todos os processos de tratamento de incidentes devem ser coordenados pela Crawford Global IT Security e/ou pelo Crawford Global Privacy Office. O indivíduo que relata o incidente pode ou não ser informado sobre o status ou os resultados da investigação, dependendo da natureza do incidente. Um Incidente só pode ser classificado como uma Violação após uma determinação de que requer ação ou notificação adicional de acordo com a lei, regulamento ou obrigação contratual. Essa classificação é determinada exclusivamente pelo Conselho Geral ou seu representante designado com base em análises independentes e/ou recomendações do Diretor de Segurança da Informação, Diretor de Privacidade ou Diretor de Informações. Até que tal determinação seja comunicada, o termo "Violação" não deve ser usado por nenhum funcionário ou outra pessoa sujeita a esta Política para descrever um Evento, Incidente de Segurança ou Incidente de Privacidade oralmente ou por escrito.

As especificidades dos Incidentes de Privacidade e Segurança não devem ser discutidas amplamente, mas devem ser compartilhadas com base na necessidade de conhecimento. Qualquer comunicação com partes externas deve ser direcionada de acordo com as políticas e procedimentos de resposta a incidentes da Crawford. Para obter informações específicas relacionadas à resposta a incidentes de segurança, consulte a "Política de resposta a incidentes de segurança cibernética e privacidade".

A perda ou roubo de um Dispositivo Emitido pela Crawford deve ser imediatamente relatado ao Crawford Service Desk ou por e-mail para Incident_Response@us.crawco.com para que eles possam iniciar a resposta adequada. Além disso, em caso de furto ou suspeita de furto, deve ser apresentado um boletim de ocorrência na jurisdição onde foi roubado.

Gerenciamento de identidade e acesso

O acesso e o uso das Informações da Crawford e dos Sistemas de Informação da Crawford devem ser restritos a pessoas devidamente identificadas, validadas e autorizadas, e devem ser fornecidos somente quando uma necessidade comercial tiver sido demonstrada e o acesso tiver sido aprovado pela administração da Crawford.

Cada usuário da Crawford deve ter um ID de usuário exclusivo e uma senha para obter acesso ao ambiente do sistema. As senhas devem ser devidamente estruturadas, alteradas e protegidas contra acesso não autorizado. As senhas nunca devem ser anotadas à mão ou armazenadas eletronicamente pelo usuário. Independentemente das circunstâncias, senhas e PINs nunca devem ser compartilhados ou revelados a ninguém que não seja o usuário autorizado. Da mesma forma, os usuários da Crawford não devem realizar nenhuma atividade com IDs de usuário, senhas ou PINs pertencentes a terceiros. Os usuários da Crawford são responsáveis por todas as atividades realizadas com seus IDs de usuário pessoais, senhas e PINs.

Os gerentes devem notificar a Crawford IT imediatamente quando os usuários da Crawford mudarem de departamento ou funções de trabalho para que os direitos de acesso ao sistema possam ser modificados para se alinharem às necessidades do sistema do novo cargo. Os gerentes devem notificar imediatamente a Crawford IT quando o cargo de um funcionário for rescindido ou as funções ou contrato de um não funcionário forem concluídos. O acesso a sistemas que suportam funções e dados empresariais financeiramente significativos deve ser objeto de uma revisão periódica do acesso. Os gerentes serão responsáveis por confirmar que o acesso ao sistema é apropriado para contas sob revisão, quando solicitado. Para obter mais informações, consulte a "Política de gerenciamento de identidade e acesso" e "Controles gerais de TI para Sarbanes-Oxley – Diretrizes de práticas recomendadas para conformidade".

Internet

A internet não deve ser usada para comunicar, transferir ou armazenar qualquer Informação Sensível ou Confidencial, a menos que a confidencialidade e integridade das informações sejam garantidas, a identidade do(s) destinatário(s) seja estabelecida e as comunicações sejam conduzidas de maneira segura. O uso de sistemas hospedados externamente ou baseados em nuvem para processar ou armazenar Informações Sensíveis ou Confidenciais deve ser revisado e aprovado com antecedência pela Crawford Global IT Security. Para mais informações, consulte a "Política de Segurança de Cloud Computing" e a "Política de Gestão de Riscos de Terceiros".

A Crawford reconhece que os funcionários podem trabalhar longas horas e, ocasionalmente, podem desejar usar a internet para atividades pessoais no escritório ou por meio de dispositivos emitidos pela Crawford ou sistemas de

informação da Crawford. Tal uso é autorizado por um tempo limitado se o uso estiver em conformidade com a lei e as políticas da Empresa em todos os momentos e não incorrer em um efeito prejudicial ao desempenho comercial do usuário ou de qualquer outro Usuário da Crawford. Os Dispositivos Emitidos pela Crawford ou os Sistemas de Informação da Crawford não devem ser usados para tentar a entrada não autorizada em uma rede ou na internet. Isso inclui a liberação deliberada de software malicioso na rede; envolver-se em jogos recreativos, obter ou distribuir materiais pornográficos e sexualmente orientados; ou realizar atividades ilegais. Os Dispositivos e Sistemas de Informação Emitidos pela Crawford são propriedade da Empresa e estão sujeitos a monitoramento de acordo com a legislação local e as políticas aplicáveis da Empresa. Na extensão máxima permitida pelas leis aplicáveis, a Crawford reserva-se o direito de monitorar o uso dos Sistemas de Informação da Crawford, incluindo qualquer coisa transmitida pelos Sistemas de Informação da Crawford ou por meio de um Dispositivo Emitido pela Crawford. Para obter mais informações. Consulte a "Política de Uso Aceitável de Crawford".

Dispositivos de propriedade pessoal

O uso de Dispositivos de Propriedade Pessoal será permitido apenas em casos estritamente limitados e com aprovação. Para obter mais informações, consulte a "Política de BYOD (Bring Your Own Device) da Crawford".

Email

O sistema de e-mail da Crawford deve ser usado predominantemente para conduzir as operações comerciais da Crawford. O uso pessoal limitado e ocasional do sistema de e-mail da Crawford é permitido, desde que o conteúdo não tenha um efeito prejudicial no desempenho comercial do usuário ou de qualquer outro usuário da Crawford. É proibido enviar informações da Crawford para uma conta de e-mail pessoal ou qualquer outra conta de e-mail que não seja da Crawford. As mensagens de e-mail devem ser acessadas apenas pelo destinatário pretendido. Crawford Os usuários devem verificar a lista de distribuição e a lista de grupos antes de enviar qualquer e-mail. Os usuários da Crawford não devem tentar obter acesso à conta de e-mail de outro usuário da Crawford ou a outros sistemas de computador para os quais não tenham acesso autorizado.

Dispositivos portáteis

Os dispositivos portáteis incluem, entre outros, laptops, notebooks, unidades USB, unidades externas, tablets e smartphones. Dispositivos emitidos pela Crawford que são portáteis (por exemplo, laptops, tablets, smartphones) ou fisicamente localizados fora de uma instalação da Crawford com proteções de segurança física (por exemplo, desktop em uma casa ou em uma área comum) devem ser criptografados.

Os usuários da Crawford estão proibidos de armazenar qualquer informação da Crawford em quaisquer dispositivos de armazenamento removíveis (por exemplo, unidade USB, CD, disco rígido externo) sem a aprovação

do supervisor do solicitante e da Crawford Global IT Security. Se um dispositivo de armazenamento removível for aprovado, as informações colocadas no dispositivo de armazenamento removível estarão sujeitas a rastreamento auditável e as informações armazenadas nele deverão ser criptografadas. Os usuários da Crawford na posse de um dispositivo portátil devem proteger fisicamente o dispositivo quando não estiver em uso (por exemplo, escritório ou mesa segura/trancada, ou permanecer na posse física da pessoa).

Mesa transparente e tela clara

As informações da Crawford não devem ser localizadas ou usadas em áreas onde uma pessoa não autorizada possa visualizar informações sensíveis ou confidenciais. Para obter mais informações, consulte a "Política de Clear Desk".

Provedores de serviços terceirizados

A Crawford deve gerenciar ativamente os riscos associados ao envolvimento com organizações externas que fornecem ou dão suporte aos Sistemas de Informação da Crawford, ou que recebem acesso às Informações da Crawford, por meio de uma estrutura formal que avalia os riscos representados por compromissos de terceiros e garante que os padrões mínimos de segurança da Crawford sejam aplicados em todos os casos. Para obter informações mais específicas, consulte a "Política Global de Gerenciamento de Riscos de Terceiros".

Segurança física

Os usuários da Crawford não devem permitir que pessoas não autorizadas passem por portas para áreas restritas ao mesmo tempo que pessoas autorizadas. Pessoas desconhecidas dentro da área segura devem ser interrogadas para garantir que tenham uma necessidade legítima de estar presentes na instalação. Os usuários da Crawford não devem abrir portas ou desativar outros dispositivos físicos de controle de acesso. O acesso físico às Áreas Controladas, como data centers, salas de servidores e armários de rede, onde a Crawford Information Systems reside fisicamente deve ser limitado apenas às pessoas que são formalmente autorizados e possuem uma necessidade comercial de acesso. Para obter mais informações, consulte a "Política de Segurança Física e Ambiental".

Contato

Para obter mais informações sobre esta Política, entre em contato com a equipe de Segurança de TI ou Risco e Conformidade de TI.

Risco e conformidade de TI	**itriskcompliance@crawco.co.uk**

Informações do documento

Nome do documento	**Política Global de Segurança da Informação**
Categoria	**Política Global**
Políticas relacionadas	**Política de Uso Aceitável** **Política BYOD (Bring Your Own Device)** **Política de Mesa Transparente** **Política de Segurança de Computação em Nuvem** **Política de Conscientização e Treinamento em Segurança Cibernética** **Política de Resposta a Incidentes de Segurança Cibernética e Privacidade** **Política de gerenciamento de riscos de segurança cibernética** **Política de Proteção de Dados e Governança da Informação** **Política de gerenciamento de identidade e acesso** **Política de Classificação e Tratamento de Informações** **Controles gerais de TI para Sarbanes-Oxley – Diretrizes de práticas recomendadas para conformidade** **Política de Segurança Física e Ambiental** **Política de gerenciamento de riscos de terceiros**
Número da versão – Data de	**Versão 7.0 – setembro de 2024**

Formulário de Revisão e Aprovação:

Política: Política Global de Segurança da Informação

Departamento	Nome e Título	Assinatura	Data
Segurança de TI	Jemin Thakkar, Chief Information Security Officer	Jemin Thakkar Jemin Thakkar (Sep 16, 2024 12:54 EDT)	09/16/24
ELA	Daniel Volk, SVP, Chief Information Officer	Daniel Volk Daniel Volk (Sep 16, 2024 12:42 EDT)	09/16/24