Política de Segurança da Informação

A reter...

- Esta política foi aprovada pela Equipa de Gestão e deve ser cumprida.
- As Políticas e Normas de Segurança da Rentokil Initial aplicam-se a Fornecedores e Parceiros quando explicitamente indicado no Cronograma de Segurança do contrato.
- A Política de Segurança da Informação suporta as visões estratégicas da Rentokil Initial ao definir a abordagem a um alto nível adotada para reduzir os riscos associados à sua reputação, finanças e operações.
- Familiarize-se com outras políticas mencionadas nesta política.
- Todos os incidentes de segurança suspeitos ou reais devem ser reportados através do ServiceNow ou Infosec.
- A informação será gerida de forma que a Rentokil Initial possa garantir o cumprimento das obrigações legais, regulatórias e contratuais.
- A Rentokil Initial reconhece que a segurança da informação é responsabilidade de todos os Colaboradores e terceiros. A Rentokil Initial está empenhada num programa contínuo de sensibilização, formação e educação para lidar com esta questão.

V1.0 junho de 2023

O que é a Política de Segurança da Informação da Rentokil Initial?

A Política de Segurança da Informação estabelece como a Rentokil Initial (RI) e os seus parceiros/fornecedores gerem e protegem a nossa informação. Procura-se explicar as responsabilidades que várias funções, cargos e indivíduos têm para garantir a confidencialidade, integridade (precisão) e disponibilidade da informação dentro da nossa organização.

Por que a Rentokil Initial necessita de uma Política de Segurança da Informação?

Uma Política de Segurança da Informação é uma prática recomendada para uma boa gestão e pelas melhores práticas da Empresa. Ela ajuda a prevenir roubo, perda e acesso não autorizado ou divulgação de ficheiros eletrónicos, documentos em papel e serviços online.

Antecedentes

A RI está empenhada em garantir que acordos de segurança eficazes sejam implementados e regularmente revistos para reduzir as ameaças e gerir os riscos em relação a: informação que a RI recolhe, cria, utiliza e armazena, dos Colaboradores da RI, dos fornecedores e parceiros da RI, os ativos e recursos físicos da RI, sistemas digitais, de TI e de comunicação, e instalações que a RI utiliza para acomodar as suas operações, pessoas e visitantes.

Âmbito

Esta política global fornece orientações para todas as políticas de segurança da informação da RI e os padrões e controlos que a sustentam.

Esta política está alinhada e é baseada na norma ISO 27000 e, em particular, com as técnicas e princípios da ISSO 27001 e nos requisitos da ISSO 27002, e será utilizada para informar a RI sobre futuras considerações de um Sistema de Gestão de Segurança da Informação. Os padrões retirados da norma ISO 27000 serão aplicados e comunicados quando necessário.

Esta política aplica-se a todos os aspectos da cibersegurança e segurança da informação, incluindo a especificação, design, desenvolvimento, utilização para armazenar, processar, instalar, operar, ligar, uso e desativação dos sistemas, serviços e equipamentos, transmitir ou receber informações.

Esta política aplica-se a todos os dados da RI e a qualquer dado que a RI esteja a processar para outros responsáveis de dados.

Objetivos da Segurança da Informação

Gestão da Segurança

Gerir e rever periodicamente os utilizadores, os processos e a tecnologia que compõem o estado de segurança da informação, com um ciclo de melhoria contínua orientado pela gestão.

Controlos Organizacionais

Assegurar que formas seguras de trabalho são definidas, compreendidas e seguidas para reduzir o risco global da segurança da informação e garantir que sejam cumpridas as obrigações legais, regulamentares e de conformidade.

Controlos Técnicos

Desenvolver e manter serviços de tecnologia da informação resilientes e adequadamente seguros, garantindo a confidencialidade, integridade e disponibilidade dos sistemas de informação e dados da RI.

Política de Segurança da Informação

Para cumprir os objetivos de segurança da informação acima mencionados, a RI garante o seguinte:

Organização e Gestão da Segurança

A liderança executiva da RI é responsável pela segurança da informação e encarregue da supervisão dos controlos e diretrizes existentes.

Os objetivos, requisitos, funções e responsabilidades de segurança da informação são supervisionados e aprovados pela liderança executiva.

Uma estrutura para a gestão da segurança da informação é definida e integrada na organização para gerir consistentemente e eficazmente os riscos de segurança da informação.

Esta estrutura garante:

- Cumprimento de todas as obrigações legais e regulamentares aplicáveis;
- Deveres e áreas de responsabilidade contraditórias são separadas para reduzir oportunidades para modificação não autorizada ou uso não intencional dos ativos da RI; são mantidos contactos adequados com as autoridades relevantes. Isso pode incluir reguladores relevantes, autoridades policiais e autoridades de supervisão. Por exemplo, o Gabinete do Comissário de Informação do Reino Unido (ICO) ou a Autoridade de Conduta Financeira (FCA);
- São mantidos contactos adequados com grupos de interesse especiais ou outros fóruns de segurança especializados e associações profissionais. Isso pode incluir grupos de interesse como o ISC2 ou o ISACA;
- A segurança da informação é considerada e tratada na gestão de projetos em toda a organização, independentemente do tipo de projeto.

A quem se aplica a Política de Segurança da Informação?

- A todos os Colaboradores da RI - que devem compreender as suas responsabilidades ao utilizar os equipamentos que contêm informação, incluindo os seus sistemas.
- A não conformidade de Colaboradores da RI com esta política pode resultar em processos disciplinares.
- Colegas da RI envolvidos no design e implementação de novas soluções tecnológicas, que devem incorporar os requisitos da política no design e construção.
- Fornecedores contratados pela RI que lidam com/acedem/processam informação sensível. Os fornecedores devem fornecer medidas de segurança e proteções apropriadas à natureza e utilização da informação. Todos os fornecedores de serviços para a RI devem cumprir e ser capazes de demonstrar conformidade com as políticas e normas relevantes da empresa.

Segurança do Colaborador

Emprego e Contratualização

Todos os Colegas e Parceiros relevantes estão sujeitos a uma avaliação prévia.
Os papéis e responsabilidades de segurança da informação (antes, durante e após o início da relação contratual) estão documentados em políticas e normas, e a conformidade com eles é uma obrigação contratual.
Existe um processo de Recursos Humanos em vigor para integração, transferência e rescisão (novos Colaboradores, transferências e saídas).
Um processo disciplinar formal e comunicado é despoletado para os Colegas que tenham violado as políticas, normas ou procedimentos de segurança da informação, ou de utilização de equipamentos.

Formação e Sensibilização

Todos os novos Colegas têm de completar a formação obrigatória em segurança da informação.
Todos os Colegas têm de completar anualmente a formação obrigatória em consciencialização de segurança da informação.

Gestão de Acesso de Utilizadores

O acesso dos utilizadores de informação é controlado, gerido e atribuído com base no princípio do menor privilégio e nos requisitos de negócio, cumprindo a Política Controlo de Acesso e as normas correspondentes.
O acesso aos sistemas e ativos de informação é regularmente revisto e gerido de acordo com os requisitos da Empresa.

Responsabilidades

O Diretor de Segurança da Informação é o proprietário responsável da Política de Segurança da Informação da RI e é responsável pela sua manutenção e revisão.
Qualquer exceção à Política de Segurança da Informação deve ser avaliada quanto ao risco e acordada pelo Diretor de Segurança da Informação.

Declarações de Política

A RI reconhece que toda a informação possui valor e estabelece nesta Política de Segurança da Informação como proteger a informação através de normas de segurança, e proteger os sistemas, equipamentos e processos que sustentam os seus usos através da aplicação de controlos e de um ambiente de controlo. Esta Política de Segurança da Informação define como alcançamos a segurança da informação através da implementação de normas e controlos de apoio para proteger a informação:

Confidencialidade - através da restrição de acesso a utilizadores autorizados;

Integridade - garantindo que a informação seja sempre precisa e completa;

Disponibilidade - garantindo que a informação esteja disponível para utilizadores autorizados quando necessário.

A RI exige que os Fornecedores que gerem, acedem e processam dados para os quais têm autoridade adotem uma abordagem proporcional e baseada em risco semelhante a segurança da informação, de acordo com as Políticas e Normas de Segurança relevantes da RI, que incorporam e aplicam os Padrões ISO 27001 e o Cyber Essentials.
A RI aplica políticas de Recursos Humanos na proteção das suas informações e exige que os Fornecedores apliquem políticas de segurança semelhantes.
A RI assegurará que a RI e os seus Fornecedores implementem e operem a segurança da informação

de acordo com as normas e procedimentos organizacionais para mitigar violações de obrigações legais, do Governo e contratuais relacionadas com a segurança da informação.

Responsabilidade dos Ativos de Informação

Identificar os ativos que contêm informação da RI e definir responsabilidades para garantir que a informação recebe um nível apropriado de proteção de acordo com a sua importância para a organização e dos nossos Clientes, bem como a sua localização.
Assegurar que a RI possui estruturas e processos adequados para permitir que o negócio compreenda a utilização e possa monitorizar os ativos que guardam informação.
A RI monitoriza e avalia sistematicamente o desempenho da segurança da informação em conformidade com as suas próprias normas e diretrizes, desenvolvendo e melhorando as políticas e normas de segurança da informação para proporcionar proteção suficiente à mesma, abordando os riscos identificados, o que é consistente com as normas e orientações da RI. Novas normas e procedimentos de segurança da informação serão comunicados regularmente aos Colaboradores e a outros intervenientes.

Responsabilidades

As Políticas e Normas de Segurança da Informação da RI proporcionam proteção adequada dos dados pessoais e dados pessoais sensíveis como resultado da implementação eficaz das seguintes responsabilidades:

Funções de Gestão e da Conformidade

- Facilitar a gestão da segurança da informação através do desenvolvimento de estruturas de gestão numa organização que orienta e gere a segurança da informação;
- Proporcionar o controlo dos riscos de segurança da informação dentro da RI a níveis aceitáveis através da gestão de riscos e do uso de marcações de proteção e outros controlos;
- Apoiar os Colaboradores da RI no cumprimento destes requisitos e garantir que os mesmos se encontram cientes das consequências da não conformidade;
- Assegurar que os Fornecedores estão cientes de que o não cumprimento desta política e de outros requisitos da mesma (que serão comunicados através do processo contratual) resultará em ações corretivas e escalonamento de acordo com os processos acordados.

Responsáveis e Fornecedores Contratados

- Garantir que todos os Colaboradores compreendem totalmente e cumprem as suas responsabilidades acordadas em relação à segurança da informação, conforme estabelecido no Código de Conduta e na Política de Utilização de Dispositivos;
- Exigir que os Fornecedores estão cientes e cumprem as suas responsabilidades em relação à informação, incluindo as responsabilidades de segurança de pessoal.

Colaboradores e Fornecedores - acesso a ativos de informação e sistemas

- Garantir que existem controlos e procedimentos documentados para o acesso a ativos de informação e que as responsabilidades de segurança tenham sido atribuídas e aceites, registando a atividade do utilizador do sistema e do serviço para determinar a responsabilidade individual;
- Garantir o uso eficaz da encriptação, especialmente quando existem interligações entre sistemas ou serviços;
- Garantir que os utilizadores sejam responsáveis pela proteção das suas informações de autenticação;

- Garantir o correto e seguro funcionamento das instalações de processamento de informação, através da regulamentação, monitorização e revisão da implementação de medidas de proteção;
- Garantir a proteção da informação em redes e em quaisquer instalações de processamento de informação de suporte, e manter a segurança da informação dentro da organização e ainda com qualquer entidade externa;
- Garantir que os dados pessoais não sejam guardados ou processados em qualquer folha de cálculo, ou sistema que não tenha sido aprovado pela RI para esse fim. Os dados pessoais só devem ser colocados em estruturas de documentos, como o Google, quando seguem os processos locais aprovados que estão em conformidade com a política de segurança da RI;
- Garantir que a segurança da informação seja integrada nos sistemas de informação ao longo de todo o ciclo de vida;
- Definir responsabilidades de segurança através de termos contratuais e requisitos para todos os Fornecedores, a fim de garantir a proteção dos ativos da organização que os Fornecedores têm acesso.

Função de Continuidade e Resiliência

Exigir que as unidades de negócio desenvolvam, implementem e incorporem uma gestão apropriada da continuidade dos negócios relativamente à segurança da informação, incluindo planos de continuidade dos negócios para sistemas e serviços críticos, com o objetivo de minimizar interrupções decorrentes de ameaças e riscos identificados.

Função de Tecnologia (através das Operações)

Exigir funcionalidade de recuperação de desastres para sistemas de segurança com base numa análise de impacto nos negócios, avaliação de riscos e cálculo de custos, em conformidade com a ISSO 27001, para restabelecer o acesso e a proteção das nossas informações.

Obrigações Legais e Regulamentares

Controlos eficazes de segurança da informação são essenciais para o cumprimento das leis no Reino Unido e em todos os outros países onde a RI atua. A legislação que impõe obrigações específicas de segurança da informação e de manutenção de registos às organizações inclui, mas não se limita a um registo legal completo e que seja mantido de:

- Computer Misuse Act de 1990.
- Data Protection Act de 2018.
- Regulation of Investigatory Powers Act de 2000.
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations de 2000.

Deteção e Resposta a Incidentes

- Devem ser implementados procedimentos para garantir que os incidentes de segurança da informação sejam detectados, geridos eficazmente e comunicados de forma atempada e adequada;
- As responsabilidades de gestão de incidentes, incluindo o requisito de reportar incidentes de segurança da informação;
- Devem ser detalhadas nos padrões, procedimentos e/ou planos adequados de resposta a incidentes;
- Procedimentos de resposta a incidentes serão implementados para reduzir o impacto dos incidentes, incluindo:

- Avaliação de incidentes, identificação da origem, comunicação e gestão de evidências.
- Os incidentes de segurança da informação devem ser registados juntamente com as conclusões aprendidas para diminuir a probabilidade de:
    - Recorrência, reduzir o risco associado e/ou melhorar as capacidades de deteção e resposta.
    - Os planos de resposta a incidentes devem ser mantidos e testados periodicamente.

Segurança Física e Ambiental

Todos os ambientes de escritório e instalações que abrigam a tecnologia da informação da empresa são protegidos por disposições de segurança física e ambiental apropriados e detalhados nas normas da segurança física.
Tais normas devem incluir disposições para abordar os controlos adequados de acesso físico e monitorização de segurança.

Gestão de Dados

- Deve ser implementada uma abordagem documentada para a identificação de ativos de informação, classificação de dados e tratamento de informações em toda a Empresa.
- Devem ser estabelecidos, implementados e mantidos padrões documentados para o uso de controlos criptográficos e gestão de chaves criptográficas, a fim de cumprir as obrigações legais, regulatórias e outras obrigações de conformidade aplicáveis.
- Deve ser estabelecido, implementado e mantido um conjunto de procedimentos para a gestão segura de suportes removíveis, conforme apropriado para a classificação dos dados neles armazenados.
- Suportes de armazenamento, dados e informações devem ser eliminados de forma segura quando já não forem necessários.

Proteção Anti-malware

Disposições de segurança anti-malware devem ser utilizadas para detectar e proteger contra a instalação, disseminação e execução de código malicioso em todos os sistemas considerados suscetíveis a ameaças de malware. A Segurança da Informação irá periodicamente reavaliar sistemas que anteriormente não foram considerados suscetíveis para determinar se tais sistemas devem ser protegidos com uma solução anti-malware.
Configurações devem ser utilizadas para impedir que utilizadores comuns desativem as proteções anti-malware sem autorização da Segurança da Informação ou de pessoal técnico designado.

Segurança do Email e Internet

Devem ser utilizadas disposições de segurança para a gateway de email e internet com o objetivo de minimizar a possibilidade de ataque e as oportunidades para que atacantes manipulem o comportamento humano através da interação com sistemas de e-mail, navegadores web ou outros sistemas de mensagens eletrónicas.
Os utilizadores não devem utilizar canais de mensagens não encriptadas ou de outra forma inseguros para a transmissão de informações sensíveis. Métodos de transmissão apropriados e seguros serão disponibilizados.

Monitorização da Segurança

Registos de auditorias que possam ajudar a detectar, compreender ou recuperar de um incidente devem ser recolhidos, geridos, protegidos e regularmente analisados de acordo com as normas estabelecidas. Os registos devem ser guardados para referência futura, de acordo com as leis,

regulamentos e requisitos de conformidade aplicáveis.

Segurança da Rede

A utilização contínua e operacional de portas, protocolos e serviços em dispositivos em rede será gerida, quer internamente quer através de outsourcing.
Políticas formais de transferência, procedimentos e controlos devem ser definidos e implementados para proteger a transferência de informações através de todos os tipos de serviços de comunicação.
Deverão ser utilizados serviços seguros em vez de serviços inseguros e não encriptados. Se os serviços inseguros tiverem de ser utilizados, serão implementadas medidas de mitigação de risco, conforme o considerado apropriado pela Segurança da Informação.

Controlo de Acessos

O acesso a todos os recursos de Tecnologia da Informação e ativos de informação será implementado com base no princípio do privilégio mínimo e nas necessidades de negócio, de acordo com a Política de Acesso e normas e procedimentos relacionados.
O acesso é controlado e gerido através de mecanismos seguros e autenticação detalhada em normas de suporte.

Cópias de Segurança e Recuperação de Desastres

Cópias de segurança de informações, software e imagens de sistemas serão guardadas, e a capacidade de restaurar dados críticos e sistemas será testada regularmente.
A resiliência será integrada nos sistemas de IT, tendo em conta os requisitos para recuperação de falhas, redundância e gestão de capacidade, conforme apropriado.
Planos de recuperação de desastres de IT serão guardados e testados periodicamente. As falhas ou lições aprendidas nos testes serão utilizadas para melhorar os planos.

Gestão de Vulnerabilidades

Todos os componentes de rede, sistemas operativos, bases de dados e aplicações devem ter suporte de segurança por parte do Fornecedor ou distribuição e estar a executar versões suportadas.
Deverão existir procedimentos documentados e implementados para identificar, gerir e prevenir vulnerabilidades de segurança em todo o ambiente de IT.

Configuração Segura de Sistemas e Desenvolvimento

Normas de segurança de IT serão aplicadas a todos os sistemas com acesso aos sistemas de informação ou dados da Empresa, incluindo dispositivos geridos, dispositivos auto-geridos, dispositivos de terceiros e dispositivos de propriedade pessoal.
Todos os sistemas associados à informação e às instalações de processamento de informação devem ser identificados e listados no inventário de ativos de IT que detalha configurações, outras infraestruturas e interligações, e são mantidos pelo proprietário ou responsável designado.
Alterações aos sistemas e serviços existentes, bem como a introdução de novos sistemas e serviços, devem ser geridas de forma a garantir que não existam impactos adversos na segurança e que são cumpridos os requisitos de segurança.
O desenvolvimento de aplicações deve seguir as normas e requisitos detalhados num ciclo de vida de desenvolvimento seguro.
A informação envolvida em serviços de aplicações que passam por redes públicas deve ser protegida contra atividades fraudulentas, litígios contratuais e divulgação e alteração não autorizada.
A informação envolvida em transações de serviços de aplicações será protegida para evitar transferências incompletas, encaminhamentos incorretos, alterações não autorizadas de mensagens,

divulgação não autorizada e duplicação ou repetição não autorizada de mensagens.
A informação envolvida em mensagens eletrónicas é adequadamente protegida, tendo em consideração todos os requisitos legais, regulamentares e específicos aplicáveis.
Os programadores de aplicações serão periodicamente treinados em programação segura para ajudar a prevenir erros de codificação que possam resultar em vulnerabilidades de segurança.

Conformidade e Excepções

A RI deverá realizar atividades adequadas de conformidade e garantia de segurança da informação para assegurar que os objetivos de segurança da informação estão a ser cumpridos.
Violações desta política podem resultar em ações disciplinares, incluindo a rescisão de contrato de trabalho ou acordo contratual, ou ação legal.
Exceções a esta política podem ser concedidas com a aprovação da gestão da Segurança da Informação e a aprovação da gestão da área de negócios afetada. Tais exceções serão concedidas ou negadas após seguir um processo para identificar limitações e riscos empresariais residuais e implementar controlos compensatórios aprovados pela liderança de IT e/ou de negócios apropriada.
A Segurança da Informação é responsável por garantir que todas as exceções sejam documentadas, guardadas em arquivo, comunicadas à gestão e divulgadas periodicamente.

Revisão e Melhoria

Esta política será publicada, comunicada e disponibilizada a todos os Colegas, contratados e parceiros relevantes.
Esta política será revista anualmente pelo Responsável pela Segurança da Informação ou quando houver uma mudança significativa no ambiente ou em um ou mais processos da Empresa. Esta revisão tem como objetivo garantir que a política permanece atual e adequada ao seu propósito, refletindo tecnologias, práticas e processos de negócios atuais, permaneça alinhada com boas práticas de segurança da informação e apoie a conformidade legal, regulatória e contratual atual.

Políticas e Documentos de Apoio

Esta Política deve ser lida em conjunto com outras políticas de apoio. Esta Política, políticas de apoio e normas de segurança relacionadas são revistas e atualizadas conforme necessário para manter um Sistema de Gestão de Segurança da Informação eficaz, a fim de satisfazer as necessidades de negócios da RI e obrigações legais:
As políticas de apoio são as seguintes:

- Política de Utilização de Dispositivos
- Política de Palavra-passe
- Política de Classificação de Dados
- Política de Sensibilização e Formação em Segurança
- Política de Gestão de Mudanças
- Política de Resposta a Incidentes
- Política de Controlo de Acesso
- Política de Gestão de Fornecedores
- Política de Retenção de Dados
- Política de Continuidade de Negócios