SEGURANÇA DA INFORMAÇÃO

UAU Ingleza

SUMÁRIO

MENSAGEM DOS SÓCIOS

Prezado colaborador,

Com o avanço da sociedade e da tecnologia, acreditamos que as informações e os dados corporativos sejam alguns dos bens mais valiosos da Ingleza e, por isso, devemos preservá-los de qualquer risco.

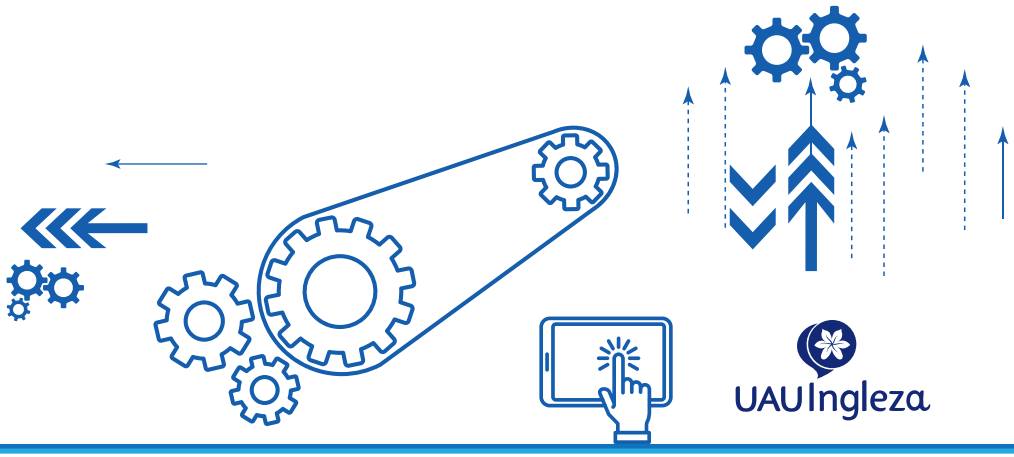
É importante reafirmar o compromisso consciente dos colaboradores em zelar pela informação, protegendo-a sempre e garantindo sua confidencialidade e integridade.

O Manual da Segurança da Informação da Ingleza traça as diretrizes para a obtenção, armazenamento, processamento, recuperação e divulgação dos dados necessários para garantir o bom funcionamento da empresa. E visa contribuir para assegurar que os colaboradores se atentem para a segurança das informações.

A gestão da segurança da informação depende do envolvimento e colaboração de cada colaborador, estagiário ou terceirizado. O cuidado com esses dados, a sua proteção e o uso adequado, são parte integrante dos negócios, mas também fazem parte da construção da história da Ingleza.

Contamos com o seu envolvimento e compromisso sempre!

Cordialmente,



INTRODUÇÃO

A informação deve ser tratada como um patrimônio, devendo ser protegida no acesso, tráfego, uso e armazenamento. Um computador/notebook ou sistema computacional é considerado seguro quando há uma garantia de que é capaz de atuar exatamente como o esperado. A expectativa de todo colaborador é que as informações armazenadas em um ambiente computacional, lá permaneçam, sem quaisquer alterações indevidas ou perdas.

QUEM DEVE CONHECER ESSA CARTILHA?

Todos os colaboradores da UAUIngleza.

PROPRIEDADE DAS INFORMAÇÕES

Todas as informações produzidas pelos colaboradores relativas às suas atividades na empresa, dentro do ambiente de trabalho ou fora dele, são consideradas de propriedade da Ingleza.

Portanto, não é permitido aos usuários realizarem cópias de informações confidenciais para uso pessoal ou de terceiros.

CONTROLE DE INFORMAÇÕES NÃO ELETRÔNICAS

Informações não eletrônicas são aquelas adquiridas em reuniões especificas, em treinamentos ou em conversas com outros
colaboradores da empresa.

Informações sigilosas devem ser respeitadas e guardadas pelos colaboradores, afim de evitar transtornos com uns com os outros e com clientes e/ou com fornecedores. Também não devem ser disseminados boatos (informações incertas ou inventadas) ou informações que, quando divulgadas com antecedência, possam causar prejuízos à empresa.

Informações adquiridas em treinamentos podem e devem ser repassadas a outros colaboradores, a fim de transmitir o conhecimento e desenvolver as equipes de trabalho.

CONFORMIDADE CONTRATUAL

Nos contratos de prestação de serviço ou transações de compra, junto aos fornecedores da empresa, é prevista uma cláusula que obriga o cumprimento da Segurança da Informação pelos contratados ou fornecedores.

Orientando-os que, quando tiverem acesso às informações confidenciais, devem proceder conforme cláusula de guarda e confidencialidade dessas informações.

CONTROLE DE INFORMAÇÕES AUDIO VISUAIS

Não é permitido realizar filmagens, gravações ou fotografar dentro da empresa, exceto nos casos em que a gerência da área tiver autorizado. Nos casos de publicidade, a diretoria de marketing deve autorizar o trabalho previamente.

Ambas as autorizações devem ser documentadas, através de e-mail com cópia para ciência aos sócios da organização e assinada também um termo de autorização que habilita as pessoas corretas referente àquela demanda. Quando houver visita técnica na empresa, o responsável por acompanhar os visitantes deve zelar para que essa regra seja cumprida.

Quando houver a necessidade de fotografar ou filmar processos completos, somente poderá ser utilizado o equipamento digital da empresa.

A visualização das câmeras da área do gerente pode ser liberada à ele através de solicitação no Help-Desk. Já as gravações das câmeras de segurança, somente serão acessadas, através de autorização da diretoria, documentada por e-mail.

COMO SE DÁ A CLASSIFICAÇÃO DA INFORMAÇÃO NA INGLEZA?

Para indicar a importância, a prioridade e o nível de proteção das informações, a Ingleza classificou as informações em 3 tipos:

Confidencial - Devem ser acessadas por um número restrito de colaboradores, a fim de ter a sua integridade e confidencialidade preservada. Se divulgadas, essas informações podem causar prejuízo financeiro, risco jurídico, desvantagem competitiva ou dano à imagem da Ingleza.

São exemplos de **INFORMAÇÕES CONFIDENCIAL:**

- Projetos.
- Projeções de produção.
- Planos de investimentos.
- Demonstrações financeiras.
- Processos judiciais.
- Formulação de produtos.
- Informação Patenteada.
- Matérias-primas e processos de Produção/Fabricação.

Interna - Informações que devem ficar restritas ao ambiente da empresa, entre os colaboradores e que não devem ser divulgadas ao público externo.

São exemplos de **INFORMAÇÕES INTERNAS:**

- E-mails.
- Quadros de avisos ou outros meios de comunicação interna.
- Procedimentos e documentos da empresa.

Pública - Informações que podem ser divulgadas para o público em geral, interno ou externo, não possuindo restrições de divulgação.

São exemplos de **INFORMAÇÕES PÚBLICAS:**

- Ramais telefônicos.
- Endereços de e-mail.
- Informações disponíveis no site e nas redes sociais da empresa.
- Notícias e comunicados divulgados à imprensa e ao mercado.
- Não necessita identificação.
- O uso do e-mail para endereços externos deve ser autorizado pelo gestor do usuário e conforme a necessidade da empresa.

COMO COMPARTILHAR INFORMAÇÕES?

Após definição do tipo de informação que está utilizando, o colaborador deve se atentar para as regras de compartilhamento delas:

TIPO DE INFORMAÇÃO	SÍMBOLO UTILIZADO	REGRAS DE COMPARTILHAMENTO
CONFIDENCIAL		Restrito à algumas pessoas. Autorização de acesso depende da análise da necessidade do colaborador. O compartilhamento com terceiros depende da autorização de um diretor ou sócio da empresa.
INTERNA		Possui acesso irrestrito dentro da Ingleza. O compartilhamento com terceiros depende da autorização de um diretor ou sócio da empresa.
PÚBLICA		Pode ser compartilhada dentro da Ingleza, com outras empresas e com o público em geral.

PROTEÇÃO DAS INFORMAÇÕES

Os critérios para definição do tipo de informação são:

		
Identificação de documentos (eletrônicos e físicos)	Utilizar o ícone "CONFIDENCIAL" - em todas as páginas e slides.	Utilizar o ícone "USO INTERNO" - apenas na capa, 1ª página ou 1° slide.
E-mail (público interno ou externo)	Deve ser enviado apenas aos destinatários autorizados. Iniciar a mensagem com o ícone "CONFIDENCIAL". Arquivos anexos devem ser protegidos por senhas.	Deve ser conferido os e-mails dos destinatários individualmente, mas nunca enviar para grupos externos.
Armazenamento (arquivos eletrônicos)	Pastas na rede ou sistemas restritos que exijam senha individual de acesso.	Pastas compartilhadas na rede.
Descarte	Material com informações confidenciais devem sempre ser destruídos antes de ser descartados. Papéis devem ser triturados ou incinerados, com o acompanhamento de um responsável pela área e discos rígidos devem ser inutilizados pelo T.I..	Conforme definido pelo responsável.

PAPEL DA T.I.

A área de Tecnologia da Informação (T.I.) é responsável pela administração dos sistemas que suportam a empresa, abrangendo compra, desenvolvimento ou manutenção deles e garantia e a segurança das informações da UAUIngleza.

É responsabilidade exclusiva do T.I.:

- Fazer o backup de todas as informações mantidas nos servidores da empresa.
- Realizar de auditorias dos computadores e controlar os softwares de monitoramento da rede.
- Avaliar a necessidade de instalação e desinstalação de quaisquer programas que sejam considerados nocivos à Segurança da Informação.
- Definir perfis dos colaboradores, com base em uma análise crítica de privilégios que não permitam a realização de atividades tidas como nocivas aos sistemas e à rede como um todo.
- Credenciar ou descredenciar contas de colaboradores.
- Garantir a segurança da informação da UAUIngleza.

UTILIZAÇÃO CORRETA DE SOFTWARES E EQUIPAMENTOS

Um software somente poderá ser instalado ou desinstalado, após avaliação e aprovação do T.I., através da abertura de chamado no HelpDesk, pelo gestor da área e de acordo com a necessidade de cada colaborador.

Antes de se ausentar do local de trabalho, o usuário deve bloquear o acesso a área de trabalho (teclas de atalho CTRL+ALT+DEL) da máquina que utiliza ou efetuar logoff do Sistema Operacional, evitando, assim, o acesso por pessoas não autorizadas.

Essa prática também evita que o colaborador perca suas informações se outra pessoa acessar, reiniciar ou desligar o computador.

Ao final do expediente de trabalho, é responsabilidade do colaborador desligar todos os equipamentos de recursos tecnológicos utilizados por ele e/ou pela área.

UTILIZAÇÃO DE MÍDIAS REMOVÍVEIS

Os drivers de dispositivos móveis, como Pen Drives e HD Externo, dentre outros, estarão desabilitados nos computadores e notebooks, no intuito de evitar a transmissão de vírus e outros arquivos indesejáveis. Em caso de necessidades específicas, a habilitação deverá ser realizada mediante abertura de chamado no Help-Desk, pelo gestor da área, justificando o motivo do uso.

Existe software de monitoramento dos computadores que utilizam dispositivos móveis.

Somente terão acesso aos recursos os Gerentes, Diretores e pessoas autorizadas formalmente pelos sócios da empresa.

Para evitar a transmissão de vírus, os celulares não deverão ser conectados aos computadores da empresa.

UTILIZAÇÃO CORRETA DE EQUIPAMENTOS CONFORME TERMOS DA TI

É responsabilidade do usuário do computador ou do notebook zelar pelo equipamento e arcar com qualquer dano causado, conforme termo de responsabilidade e confidencialidade, enquanto ele estiver sob sua utilização. Se for necessária a substituição de peças, elas devem ser substituídas conforme características do equipamento original, com o acompanhamento do TI.

O notebook pode ser retirado da empresa para uso do colaborador, durante o horário de trabalho, com autorização do gestor imediato.

A autorização deve ser documentada através de e-mail. Os cargos de Gerência e Diretoria não precisam de autorização prévia.

Nas férias do colaborador, o notebook utilizado por ele, deve ser mantido em local seguro, pelo gestor da área.

ACESSO SEGURO ÀS PASTAS DE TRABALHO NA REDE

Todos os arquivos e programas devem ser mantidos no servidor, onde existe um sistema de backup diário e confiável. Após desligamento do computador ou notebook, os documentos salvos na área de trabalho serão removidos automaticamente. O T.I. não recupera documentos que não estiverem salvos no servidor.

Os usuários devem ser cuidadosos ao criar e/ou remover arquivos em pastas no servidor, para evitar que dados importantes sejam perdidos ou o comprometimento do desempenho e do funcionamento delas.

HORÁRIO DE ACESSO AOS RECURSOS DA INFORMAÇÃO

O horário de acesso à rede e softwares da empresa é restrito ao horário da jornada de trabalho do colaborador, assim como o acesso dos estagiários e terceiros autorizados é restrito ao horário contratual.

Para que o T.I. libere acesso aos recursos da informação após o horário definido, é necessária a solicitação ao gestor imediato do colaborador, por Help-Desk.

O bloqueio das informações após horário definido, abrangerá todos os instrumentos de trabalho disponíveis na Ingleza, tais como sistemas, e-mails, internet, documentos e acesso a rede, exceto diretores e gerentes.

DEFINIÇÃO DE USUÁRIOS E SENHAS

O login do usuário será definido da seguinte forma: sempre o primeiro nome, seguido do último sobrenome e em caso de colaboradores com o mesmo nome, um outro sobrenome pode ser utilizado. A regra somente pode ser alterada a pedido justificável do colaborador. Para login de computador e sistemas não poderão ser criados usuários genéricos (nome de setor).

Cada usuário será identificado através de uma senha, pessoal e intransferível, que o qualificará como responsável por todas as ações tomadas através dela.

A senha deverá ser obrigatoriamente trocada pelo usuário no primeiro acesso a cada 3 meses.

É exigência que a formação da senha tenha letras e números e para alterá-la, a nova senha não pode ser igual às cinco últimas digitadas anteriormente.

REGRAS DE LIBERAÇÃO DE ACESSO ÀS PASTAS NO SERVIDOR

A liberação de acesso às pastas (para alteração ou consulta) deve ser aprovada e registrada no Help-Desk pelo gestor do colaborador, de acordo com as necessidades dele. Caso haja necessidade de liberação de uma pasta que não pertence ao setor desse colaborador, o gestor da área à qual a pasta pertence também deve autorizar a liberação, através de registro de chamado no Help-Desk.

Quando um colaborador é transferido para outra área, é responsabilidade de seu gestor imediato garantir o acesso aos sistemas e a outros controles de segurança necessários e retirar os acessos desnecessários.

REGRAS PARA PERSONALIZAÇÃO DE SISTEMAS

É necessário que o requerente documente todas as necessidades de personalização dos sistemas da empresa que afetarão a sua área, através de abertura de chamado Help-Desk, com cópia para aprovação do gestor imediato. Quanto à validação das personalizações realizadas, quando necessário, as áreas indiretamente envolvidas também devem participar, fazendo a validação noHelp-Desk.

Os testes das personalizações realizadas devem ser feitos em base de testes e nunca na base oficial e validados pelo gestor da área.

RESPONSABILIDADE QUANTO AOS ACESSOS AO BANCO DE DADOS

Cada usuário é responsável pela confiabilidade dos dados gerados ou alterados por ele. Caso seja percebido um erro em dados recebidos ou gerados, o usuário deve comunicar imediatamente o problema ao seu gestor para correção.

Não é permitido o uso de qualquer tipo de programa ou comando designado a interferir na sessão de qualquer conta, servidor ou rede.

Somente tem acesso ao banco de dados da empresa os colaboradores do T.I., sendo cada um deles com permissões distintas, conforme suas necessidades e autorização junto ao gestor da área.

USO SEGURO DO E-MAIL

Não é permitido o cadastramento do e-mail corporativo em sites que não sejam de interesse da empresa, para evitar recebimento de “spams”, vírus e outros.

Não é permitido ao colaborador, o acesso ao e-mail corporativo, fora do horário de trabalho, exceto os colaboradores que ocupam cargo de supervisor, gerente e diretor.

Não é permitido enviar e-mails que contenham piadas, correntes, mensagens de autoajuda ou outro conteúdo que não seja referente ao trabalho. O envio de e-mails para todos os usuários da empresa é restrito às áreas de Comunicação e Marketing, Recursos Humanos e Tecnologia da Informação.

O usuário deve fazer manutenção das caixas de e-mail, evitando acúmulo de mensagens desnecessárias, principalmente com anexos.

É obrigatória a utilização de assinatura padrão da UAUIngleza nos e-mails para todos os colaboradores.

Para garantir a segurança e a integridade das informações geradas pela UAUIngleza, auditorias no e-mail, nos computadores e notebooks dos usuários, serão realizadas pelo Time de segurança da informação e o Gestor de T.I. periodicamente.

ACESSO À INTERNET

A internet deve ser utilizada como complemento às atividades do setor e como ferramenta para buscar informações que venham agregar valor às necessidades da empresa.

Para que um usuário tenha acesso à internet, seu gestor imediato deve fazer a abertura de um chamado no Help-Desk, justificando a necessidade.

Antes da liberação, o usuário deve assinar o Termo de Responsabilidade e Confidencialidade e cumprir as regras de limitação de acesso definidas no documento.

É utilizado na empresa um mecanismo de Firewall, que monitora todo o tráfego da rede. Diariamente, é gerado um relatório contemplando todos os sites navegados por usuário.

Não é permitido utilizar os recursos da empresa para efetuar downloads ou distribuição de software ou dados ilegais.

Não é permitido downloads e transferências de arquivos de vídeos, sons e/ou imagens gráficas não relacionados aos interesses da empresa. Não é permitido divulgar informações confidenciais/sigilosas da empresa em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas na forma da lei.

Não é permitido utilizar serviços de streaming, tais como: Youtube, rádios on-line e afins, sem fins profissionais, exceto para as áreas específicas, diretoria e gerência.

É inadmissível, passível de punição e cabível de bloqueio imediato do acesso, as tentativas de:

- Visualizar conteúdo pornográfico ou obsceno;
- Distribuir, interna ou externamente, dados considerados impróprios/inadequados;
- Acessar sites que defendam atividades ilegais, que possuam informações difamatórias ou que incitem o preconceito;
- Enviar material ofensivo ou de assédio para outros usuários;
- Executar atividades que comprometam a Segurança da Informação na empresa;
- Introduzir, de qualquer forma, arquivos que comprometam o uso da internet ou perturbem o andamento das atividades, e;

O acesso ao Wifi de uso exclusivo para a internet é autorizado somente aos gerentes, diretores e visitantes. A senha de acesso é alterada periodicamente, conforme as regras de segurança do T.I. As senhas dos visitantes serão geradas Tickets “Hora, Dia e Semana”. Demais acessos deverão ser solicitados pelo gestor imediato pelo Help-desk.

COMO FUNCIONAM AS LEIS ASSOCIADAS À SEGURANÇA DA INFORMAÇÃO?

A UAUIngleza, seus colaboradores e todos aqueles que estejam envolvidos com suas atividades devem submeter-se não somente ao Manual de Segurança da Informação, como também às leis vigentes, estatutos, regulamentos ou contratos aos quais a empresa está sujeita.

Ficam sujeitas às disposições legais, regulamentares e estatutárias, a administração, exploração, transmissão ou utilização das informações de propriedade da UAUIngleza.

A quebra da segurança das informações da UAUIngleza pode ter consequências que vão além do ambiente empresarial. Existem informações que, se comprometidas, podem trazer consequências legais para a empresa e para o usuário envolvido.

DESCUMPRIMENTO DAS REGRAS

O descumprimento das regras estabelecidas no Procedimento de Segurança da Informação poderá ser passível de penalidades.

ESCLARECIMENTOS E DENÚNCIAS

Dúvidas de interpretação, situações não previstas e denúncias de descumprimento desse procedimento devem ser apresentadas à liderança ou ao canal de Ouvidoria.

Toda denúncia recebida pela Ingleza será tratada com confidencialidade.

PROCEDIMENTO DE REFERÊNCIA

As demais informações sobre Segurança da Informação podem ser consultadas no Manual de Segurança da Informação (PGQ - MANUAL SEGURANÇA DA INFORMAÇÃO), disponível no servidor de arquivos da UAUIngleza.

UAU Ingleza