01 DETALHES

Título: Política de Segurança da Informação
Original Date & Place: Sao Paulo, 12 de Janeiro, 2018
Last Update: 1º Abril, 2018
Alcance: Obrigatório a todos os procedimentos internos. Obrigatório a todos os colaboradores, em todos os segmentos, independente de faixas salariais, cargos, tempo de empresa, ou outras condições.

02 OBJETIVOS DESTA POLÍTICA

O propósito desta política é permitir que nossa empresa e seus indivíduos acessem e processem informação de maneira legal, segura, eficiente e eficaz. Ela permite aos indivíduos ter acesso à informação necessária para um trabalho eficiente, ao mesmo tempo que protege informação sensível e a propriedade intelectual de maneira segura, evitando perdas financeiras aos investidores, parceiros e à todas as partes interessadas. Nossas diretrizes são:

(1) Estabelecer o papel de nossa informação para poder cumprir os objetivos organizacionais;

(2) Gerenciar informação de maneira segura, tratando-a como um ativo organizacional em nossa empresa, providenciando-a de maneira atempada, apropriada, precisa e atualizada onde é necessária;

(3) Disponibilizar informação tão rápido quanto possível;

(4) Tomar medidas cabíveis para proteger informações, avaliando e gerenciando os riscos pertinentes para manter sua qualidade, confidencialidade, integridade e disponibilidade;

(5) Criar uma cultura de gestão de informação onde a equipe assuma responsabilidade pessoal no manejo da informação e seja aderente com todos os requisitos institucionais;

(6) Encorajar a adoção das melhores práticas na gestão da informação como descrito neste guia.

Por meio destas doutrinas, temos como objetivo tratar a informação como um ativo organizacional permitindo que ela seja acessada por quem a precisa para cumprir suas tarefas. Entendemos que a informação é crítica na criação de valor e estamos comprometidos em assegurar que todos estejam sempre cientes e respeitosos em relação à confidencialidade da informação que produzem, compartilham ou recebem.

03 CLASSIFICAÇÃO DA INFORMAÇÃO

As informações podem ser classificadas de acordo com a sensibilidade de seus dados e potencial para criar danos financeiros e/ou intangíveis negativos. As informações sempre

carregam algum risco e podem prejudicar o interesse da empresa ou de indivíduos e devem ser adequadamente tratadas, armazenadas e transmitidas. O objetivo da classificação da informação é garantir que a informação seja compartilhada somente com as pessoas apropriadas em circunstâncias apropriadas, de modo a manter a propriedade intelectual e as informações estratégicas sob controle. O objetivo da classificação de informações é:

(1) Proteger as informações confidenciais do acesso não autorizado. No curso normal dos negócios, certas informações devem permanecer confidenciais. Exemplos de tais informações incluem o orçamento anual, arquivos de recursos humanos ou demonstrações financeiras. A aplicação de uma classificação e práticas adequadas de segurança pode proteger contra o acesso não autorizado a informações confidenciais;

(2) Proteger a propriedade intelectual. Temos investimentos significativos em propriedade intelectual. O *Framework* de Gestão da Informação exige que esses investimentos sejam protegidos para beneficiar a empresa, usuários e investidores. Práticas de segurança adequadas são necessárias para garantir um nível adequado de proteção.

Existem 3 (três) níveis de informação na organização. Cada nível requer um conjunto específico de precauções a serem tomadas ao lidar com seu manuseio, armazenamento e transmissão.

NIVEL	DESCRIÇÃO	RISCOS	REQUISITOS
NIVEL 1 (L1)	IRRESTRITO - Informações que são criadas no curso normal dos negócios, que provavelmente não causarão dano.	Sem impactos. Se perdido, mudado ou negado não resultaria em risco legal ou financeiro.	Deve ser aderente aos requisitos de *branding* da empresa.
NIVEL 2 (L2)	RESTRITO - Informações sensíveis em ambiente externo à empresa e que podem afetar os níveis ou desempenho do serviço, ou resultar em baixos níveis de perda financeira. Inclui informações financeiras ou detalhes sobre operações.	Poderá oferecer vantagem competitiva a terceiros Interrupção de négócios se não estiver disponível.	Não pode ser compartilhado ou transferido para além da empresa.
NIVEL 3 (L3)	CONFIDENCIAL – A informação que é sensível e pode causar séria perda de privacidade, vantagem competitiva, perda de confiança, danos aos investidores, parcerias, relacionamentos e reputação não podem ser compartilhadas ou transferidos para além da empresa.	Perda de reputação ou vantagem competitiva . Perda de segredos comerciais ou propriedade intelectual. Perda financeira.	Não pode ser transferido sem autentificação (isto é, o uso de um *log*, criptografia ou senha pessoal ou chave) Exigir *MoU* (*memorandum of understanding*) ou *NDA* (*non disclosure agreement*) assinado antes de transmissão.

04 MANUSEANDO A INFORMAÇÃO

É importante considerar quanto a informação confidencial é necessária antes de divulgá-la e apenas o mínimo necessário deverá ser compartilhado. Há três processos necessários para lidar com informações:

Rotulagem: classificar informações de acordo com seu potencial de risco;

Armazenamento: fornecer armazenamento e mídia apropriadas para a informação que deve ser compartilhada;

Transmissão: avaliar como transmitir a informação de acordo com sua classificação e conteúdo.

A tabela abaixo oferece regras gerais para garantir que a melhor governança para as informações esteja sendo atendida:

NÍVEL	CONDIÇÃO	ARMAZENAMENTO	TRANSMISSÃO	EXEMPLOS
NÍVEL 1 (L1)	IRRESTRITA	Não é necessário armazenamento especial .	Deve ser aderente aos requisitos de *branding* da marca antes de qualquer publicação.	Comerciais da empresa, *teasers*. relatórios públicos, material de mídia social.
NÍVEL 2 (L2)	RESTRITA	Todas as mídias devem estar sob uma zona segura (ou seja, devem exigir acesso autorizado, como o servidor da empresa).	Não pode ser compartilhado ou transferido fora da empresa ou dos dispositivos da empresa. Requer rotulagem .	Planos de gestão, orçamentos. Demonstrações financeiras.
NÍVEL 3 (L3)	CONFIDENCIAL	Todas as mídias devem ser armazenadas de forma segura passíveis de auditoria (se mídia física) ou em uma zona de alto nível, com acesso restrito.	Não pode ser transferido sem autenticação (ou seja, criptografia e senha pessoal ou chave). Exigir *MoU* ou *NDA* assinado antes de transmissão.	Planos de negócios e anexos, Contratos sociais, registros pessoais, dados do usuário.

05 IDENTIFICAÇÃO & RASTREIO DE ACESSOS

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a Catwalk e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade). Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

O usuário, vinculado a quaisquer dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal). Todo e qualquer

dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir *login* de uso compartilhado por mais de um colaborador, a responsabilidade perante a Catwalk e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

É proibido o compartilhamento de *login* para funções de administração de sistemas.

Somente usuários autorizados poderão criar identidades digitais para serviços utilizados pela empresa, em seus sistemas internos ou externos. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 8 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo). Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente, além de um dispositivo físico gerador de *token* de autenticação. É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras. Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

Os sistemas críticos e sensíveis para a instituição e os *logins* com privilégios administrativos devem possuir sistema de autenticação dupla, em dispositivo físico.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, a administração deve tomar providência destas ações. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares. Usuários que não efetivem acesso às suas respectivas contas em período superior a 14 (quatorze) dias poderão ter suas senhas bloqueadas pelo administrador do sistema.

O CTO ficará de posse e administração do coordenador de infraestrutura e Controle de Contas Administrativas. O acesso é feito através do uso de e-mail cadastrado, senha e *token* de autorização que é enviado para o dispositivo físico desta pessoa.

06 PRECAUÇÕES DE SEGURANÇA

Algumas diretrizes são gerais e aplicam-se a todas as informações e seu armazenamento e processamento, e merecem destaque:

Senhas: Não criar senhas com menos de 8 caracteres. Adicione pelo menos um número e uma letra maiúscula. Não compartilhe senhas. Não escreva senhas em mídia eletrônica, como e-mails, arquivos ou equivalentes;

Acesso WIFI: Não acesse WIFI em locais públicos com nenhum dos dispositivos da empresa. Use o ponto de acesso pessoal do seu celular para acessar a internet;

Dispositivos USB: Não insira dispositivos USB em dispositivos da empresa, a não ser que seja um dispositivo USB autorizado. Não misture documentos pessoais e da empresa em dispositivos USB autorizados;

E-mails: O envio de e-mails para contas pessoais é estritamente proibido. Não compartilhe e-mails e não imprima e-mails. Use uma senha diferente em sua conta de e-mail pessoal. Não configure "resposta a todos" como padrão na sua configuração de e-mail. Verifique o endereço do remetente do e-mail para evitar confusão;

Notebooks: Não deixe computadores sem vigilância em qualquer lugar público;

Mídia Física: Não deixe dispositivos sem vigilância, não deixe informações confidenciais espalhadas sem vigilância, como mensagens telefônicas, impressões de computador ou planos de gerenciamento;

Contas: Não deixe as contas conectadas quando sair. Não faça *login* em computadores públicos;

Conversas e Reuniões: Não mantenha conversa com informações confidenciais em locais públicos ou lugares lotados, como cafeterias ou restaurantes. Não faça apresentações na mesa em tais lugares.

Os colaboradores podem ser responsabilizados pessoalmente por uma violação de confiança se estas diretrizes não forem seguidas.

07 *COMPLIANCE*

Um canal de comunicação aberto está aberto para garantir dúvidas, sugestões e reclamações sobre esta política.

falecom@mycatwalk.com

Devemos investigar quaisquer inquéritos e relatórios não conformes, resultando em um relatório no prazo máximo de 14 (quatorze) dias, incluindo uma resposta ao inquiridor.

Devemos manter um banco de dados aberto para registrar todas as perguntas e relatórios, incluindo eventos e acompanhamentos não conformes, sua descrição, a solução e toda a responsabilidade relacionada.

08 VALIDADE

Esta política é válida e exigível através de todas as nossas operações por meio do *status* obrigatório e com prazo indeterminado.