omnisblue

POLÍTICA DE SEGURANÇA APLICADA A PESSOAS

Omnisblue | Departamento de Infraestrutura

1. Histórico de revisão do documento

Abaixo são registrados as versões e atualizações deste documento.

Versão	Data	Autor	Alterações
1.0	07/02/2023	Daniel Zaitz	Versão inicial do documento.

2. Objetivo

Esta política tem como objetivo definir controles para que os colaboradores entendam suas responsabilidades de acordo com os seus papéis dentro da empresa e que deixem a organização ou mudem de função de forma ordenada, reduzindo assim o risco de roubo, furto, apropriação indébita, fraude ou mau uso dos recursos de informação da OMNISBLUE.

3. Definições

Colaborador – funcionários, trabalhadores temporários, estagiários, aprendizes e quaisquer mão-de-obra de terceiros que executem suas atividades de forma não eventual dentro das instalações da OMNISBLUE ou mediante o uso dos recursos de informação da OMNISBLUE.

- **Informação** - Recursos de informação são definidos como qualquer dado criado, coletado, comunicado, usado ou observado por qualquer usuário de informação durante o seu período empregatício ou relacionamento com a OMNISBLUE.
- **Informação sensível** – Qualquer informação de propriedade da OMNISBLUE que esteja classificada como níveis “confidencial” ou “proprietária” definidos na POL07 – Política de Classificação da Informação.

4. Papéis e responsabilidades

a) As responsabilidades pela segurança das informações da OMNISBLUE devem ser incluídas:
   i. No termo de confidencialidade e responsabilidade assinado obrigatoriamente pelos funcionários no momento da contratação;
   ii. No contrato assinado pela empresa responsável pelos terceiros ou no termo assinado pelos próprios terceiros quando da solicitação de acesso a recursos de informação da OMNISBLUE

b) Devem ser claramente definidos e comunicados os papéis e responsabilidades pela segurança da informação para pessoas que não estejam engajadas por meio do processo de contratação da organização, como, por exemplo, através de uma organização terceirizada;

c) Os papéis e responsabilidades pela segurança da informação devem incluir requisitos para que os colaboradores ajam de acordo com as políticas de segurança da informação da organização, definição de responsabilidades pela classificação da informação, requisitos para proteção dos ativos contra acesso não autorizado, divulgação, modificação, destruição ou interferência e atribuição de responsabilidades para os casos de violação;
d) Os colaboradores devem entender e assinar os termos e condições de sua contratação para o trabalho;
e) Os termos e condições de trabalho devem incluir:
    i. Que todos os colaboradores assinem um termo de confidencialidade ou de não divulgação antes de obterem acesso aos recursos de processamento da informação da OMNISBLUE;
    ii. Definição das responsabilidades dos colaboradores pelo tratamento de informações recebidas de outras companhias ou de partes externas;
    iii. Definição das responsabilidades da organização pelo tratamento das informações pessoais, incluindo informações pessoais criadas como resultado de, ou em decorrência da, contratação com a organização;
    iv. Definição das responsabilidades sobre as informações e ativos da empresa, que se estendam para fora das dependências da organização e fora dos horários normais de trabalho;
    v. Ações a serem tomadas com relação aos colaboradores que desrespeitarem os requisitos de segurança da informação da organização.

5. Seleção

a) A área de Recursos Humanos deverá ter um processo de controle para contratação de novos funcionários e de fornecedores de mão-de-obra. Tal processo deverá contemplar os seguintes itens:
    i. Confirmação das qualificações acadêmicas e profissionais;
    ii. Confirmação de referências pessoais e profissionais;
    iii. Confirmação de experiência em empregos anteriores; e
    iv. Quando essencial à natureza da função e na medida em que for autorizado pela legislação brasileira, a verificação de antecedentes criminais e de informações de crédito.
b) A área de Recursos Humanos deve zelar pela observância dos quesitos de segurança citados nos itens 3 e 4 desta política, no processo de contratação de funcionários, trabalhadores temporários, estagiários, aprendizes e quaisquer mão-de-obra de terceiros que executem suas atividades de forma não eventual, dentro das instalações da OMNISBLUE ou mediante o uso dos recursos de informação da OMNISBLUE. Para a contratação de trabalhadores temporários, o contrato de serviço deve especificar claramente as responsabilidades da agência pela seleção e os procedimentos de notificação que devem ser seguidos se a seleção não for devidamente concluída ou quando os resultados obtidos forem motivo de dúvidas ou preocupações. Do mesmo modo, os acordos com terceiros devem especificar claramente todas as responsabilidades e procedimentos de notificação para seleção.

6. Responsabilidades dos Gestores

a) É responsabilidade dos gestores assegurar que os membros da sua equipe:
    i. Estão adequadamente instruídos sobre suas responsabilidades e papéis pela segurança da informação antes de obter acesso às informações sensíveis ou aos sistemas de informação;
    ii. Recebam o Manual de Segurança da Informação e cumpram as determinações contidas no mesmo;
    iii. Forneçam tempo de trabalho suficiente para que os colaboradores se familiarizem com as políticas de segurança, procedimentos e maneiras relacionadas de realizar suas tarefas;
    iv. Atinjam um nível de conscientização sobre segurança da informação que seja adequado para os seus papéis e responsabilidades dentro da organização;
    v. Estejam cientes das atualizações das políticas de segurança publicadas periodicamente pela segurança da informação;
    vi. Atendam aos termos e condições de contratação.

7. Educação e Treinamento

a) Durante o processo de contratação, ou até o primeiro dia de trabalho, todos os novos colaboradores da OMNISBLUE devem receber uma cópia do Manual de Segurança da Informação, receber treinamento de integração e devem ser conscientizados do papel da segurança em suas funções de trabalho;
b) Os usuários não devem receber acesso aos sistemas de informação da OMNISBLUE a menos que:
    i. Tenham lido as políticas de segurança relevantes para suas funções de trabalho;
    ii. Tenham retornado ao RH o termo de recebimento e responsabilidade contido no Manual de Segurança da Informação devidamente assinado;
c) Os treinamentos de segurança da informação devem ser adequados e relevantes para os papéis, responsabilidades e habilidades da pessoa, e devem incluir informações sobre conhecimento de ameaças, quem deve ser contatado para orientações sobre segurança da informação e os canais adequados para relatar os incidentes de segurança da informação;

8. Processo Disciplinar

Quando comprovado pela área de segurança da informação que um colaborador cometeu uma violação de segurança da informação, este deve ser submetido a penalizações que devem levar em consideração fatores como a natureza e a gravidade da violação e o seu impacto no negócio, se o infrator é reincidente, se foi adequadamente treinado, as legislações relevantes, os contratos de negócio e outros fatores conforme requerido.

a) O processo para o funcionário deve prever sanções em uso pela OMNISBLUE regidas pela CLT e Código Civil, incluindo, mas não se limitando a:
    i. Comunicação do incidente ao usuário e ao gestor, pela área de segurança;
    ii. Suspensão temporária dos acessos, também pela área de segurança;
    iii. Advertência trabalhista formal, aplicado pela área de Recursos Humanos;
    iv. Suspensão sem remuneração aplicada pela área de Recursos Humanos;
    v. Término do contrato de trabalho por justa causa;
    vi. Solicitação de indenização pelos danos provocados em razão da violação da segurança da informação.
b) No caso de prestadores de serviço, devem ser previstas punições no contrato de prestação de serviços com a empresa contratada para o caso de violações de segurança da informação, incluindo, mas não se limitando a:
    i. Comunicação do incidente ao usuário e ao gestor, pela área de segurança;
    ii. Suspensão temporária dos acessos, pela área de segurança;
    iii. Substituição do infrator por outro recurso, solicitado pela Diretoria Executiva gestora do contrato;
    iv. Rescisão do contrato com a empresa contratada, incluindo a aplicação de multas contratuais processos civis, de acordo com a gravidade da violação, solicitado pela Diretoria Executiva gestora do contrato;
    v. Solicitação de indenização pelos danos provocados em razão da violação da segurança da informação.

9. Encerramento de contrato ou mudança de área

a) Colaboradores com acesso a informações sensíveis, quando desligados da empresa, devem assinar um termo de compromisso de sigilo. O período de compromisso de sigilo deve constar deste, sendo determinado de acordo com as necessidades de negócio da empresa;
b) O processo de encerramento de atividades deve contemplar a devolução de todos os equipamentos, documentos corporativos e softwares entregues à pessoa durante o período de contratação. Outros ativos da organização, tais como dispositivos de computação móvel, cartões de créditos, cartões de acesso, softwares, manuais e informações armazenadas em mídia eletrônica também precisam ser devolvidos;
c) Todos os direitos de acesso (lógico e físico) de todos os colaboradores às informações e aos recursos de processamento da informação da OMNISBLUE devem ser retirados após o encerramento de suas atividades; É responsabilidade dos gestores reportarem as mudanças de atividade dos colaboradores para que seja efetuada a retirada de todos os direitos de acesso (lógico e físico) que não forem aprovados para o novo trabalho;

d) Caso o colaborador que esteja saindo tenha conhecimento de senhas de contas que permaneçam ativas, estas devem ser alteradas após o encerramento das atividades, mudança do trabalho, contrato ou acordo;
e) Nos casos em que um colaborador compre um equipamento da organização ou use o seu próprio equipamento pessoal para atividades da empresa, procedimentos devem ser adotados para assegurar que toda a informação relevante seja transferida para a OMNISBLUE e que seja apagada de forma segura do equipamento em questão.

Comentários Gerais

Todo e qualquer comentário relativo aos procedimentos descritos neste documento devem ser encaminhados à área de Infraestrutura da OMNISBLUE: