Política de Mesa e Tela limpa

Hospital São Marcos

Junho 2025

Sumário

HOSPITAL
SÃO MARCOS

1. Visão Geral

A Política de Mesa e Tela Limpa é essencial para assegurar que materiais sensíveis e informações confidenciais sejam removidos das áreas de trabalho e armazenados em local seguro sempre que não estiverem em uso, ou quando o colaborador se ausentar da sua estação. Essa prática é uma medida eficaz para minimizar riscos de exposição ou acesso indevido a dados sigilosos, protegendo informações de pacientes, documentos internos e demais registros confidenciais. Além disso, a política reforça a importância da conscientização contínua de todos os profissionais quanto à segurança das informações, promovendo uma cultura organizacional focada na segurança e na responsabilidade no tratamento de dados.

2. Objetivo

O objetivo desta política é estabelecer os requisitos mínimos para a manutenção de uma “Mesa e Tela Limpa” assegurando que informações confidenciais/críticas sobre pacientes, funcionários e demais partes envolvidas, sejam mantidas em áreas seguras e trancadas, fora do alcance de pessoas não autorizadas. Além de estar alinhada com as normas ISO 27001/17799, essa política também faz parte dos controles básicos de Privacidade e Segurança da Informação.

3. Escopo

Esta política se aplica a todas as pessoas que desempenham atividades nas dependências do hospital São Marcos, incluindo, mas não se limitando a: funcionários, estagiários e prestadores de serviços.

4. Diretrizes da Política

Os colaboradores do Hospital São Marcos devem estar cientes de todas as diretrizes desta política, uma vez que são responsáveis por diversas informações confidenciais e devem zelar pela sua proteção.

As lideranças e gestores desempenham um papel fundamental nesse processo, atuando como ponto de referência para suas equipes e assegurando que todos compreendam e sigam as práticas de segurança estabelecidas.

Todos os colaboradores, estagiários, prestadores de serviços e demais profissionais que atuam no Hospital São Marcos devem participar de programas de conscientização sobre a

importância de manter mesas e telas limpas, como forma de proteger informações sensíveis e preservar a segurança dos dados.

Registros de pacientes, informações clínicas, administrativas e relacionadas à conduta profissional devem ser rigorosamente protegidos contra acessos não autorizados, conforme as normas de privacidade e segurança da informação.

4.1. Mesa Limpa

É importante definir e aplicar regras de mesa limpa para documentos impressos e mídias de armazenamento removível, bem como regras de tela limpa para recursos de tratamento de informações, por exemplo:

- Anotações, recados, lembretes, mídias de computador e quaisquer informações relacionadas a pacientes ou profissionais não devem ser deixados sobre as mesas, nem fixados em paredes, divisórias ou nos monitores dos computadores.

- Qualquer informação restrita ou sensível deve ser removida da mesa e armazenada em local seguro quando não estiver sendo utilizada, quando o proprietário da informação se ausentar da mesa e ao final do dia.

- Armários e gavetas contendo informações sensíveis ou restritas devem ser mantidos fechados e trancados quando não estiverem em uso.

- As senhas não devem ser anotadas em nenhum local físico, como quadros brancos ou notas adesivas.

- Impressões contendo informações restritas ou sensíveis devem ser realizadas somente em casos de extrema necessidade e removidas imediatamente da impressora. Isso ajuda a garantir que documentos confidenciais não fiquem disponíveis para qualquer pessoa.

- Nenhum quadro deve conter informações restritas ou sensíveis anotadas.

- Documentos físicos, agendas e cadernos de anotações devem ser guardados em local seguro quando não estiverem em uso, especialmente fora do horário do expediente.

- Toda a área de trabalho deve estar sempre limpa e organizada, essa ação torna mais eficiente a divisão entre os documentos que possuem informações sensíveis ou não.

- O descarte dos documentos restritos, confidenciais e/ou sensíveis deve ser feito com atenção utilizando métodos apropriados e descartando-os em locais designados seguros.

- Chaves utilizadas para acessar informações restritas ou sensíveis não devem ser deixadas sobre a mesa, armário, gaveteiro ou introduzida na fechadura.

4.2. Tela Limpa

Manter a tela limpa é crucial para a segurança das informações. Isso assegura que, quando os dispositivos não estão em uso, suas telas permaneçam protegidas contra acessos não autorizados e reduz o risco de exposição de dados confidenciais, por exemplo:

- Estações de trabalho, quando não compartilhadas, devem sempre ser bloqueadas ou ter o *logoff* realizado quando o colaborador não estiver utilizando, mesmo que por um curto período.

- Os computadores e sistemas devem ser configurados com um recurso de tempo-limite ou encerramento de sessão automáticos.

- Telas de computadores não devem ser visíveis para pessoas não autorizadas ou para o público.

- Todos os sistemas que solicitam credenciais de acessos como *e-mail*, por exemplo, devem ser feitos *logoff* antes do desligamento da máquina. Assim como não habilitar o “lembrar de mim” ou “lembrar senha” que são facilitadores de acesso não autorizado.

- O uso de dispositivos USB deve ser bloqueado. Qualquer mídia que possa conter informações sigilosas deve ser criptografada.

- Os dispositivos eletrônicos devem passar por supervisão para garantir que não sejam utilizados de maneira indevida ou para acessar informações confidenciais.

- Senhas e credenciais de acessos jamais devem ser compartilhadas com terceiros, mesmo que eles sejam de “confiança”.

- As senhas devem ser armazenadas exclusivamente em um cofre de senhas para prevenir o acesso não autorizado a contas e informações pessoais.

- Estabelecer e comunicar regras e orientações para a configuração de alertas nas telas (por exemplo, desligar os novos alertas de e-mail e mensagens, se possível, durante apresentações, compartilhamento de tela ou em área pública).

5. Conformidade

5.1. Gestão de Conformidade

A equipe de segurança da informação verificará a conformidade com esta política através de vários métodos, incluindo orientações periódicas, auditorias internas e *feedback* ao proprietário da política.

5.2 Exceções

Qualquer exceção deverá ser previamente aprovada pelo time de Segurança da Informação e receber a aprovação do Comitê de Segurança da Informação.

5.3 Não Conformidade

O colaborador que violar esta política está ciente de que tal conduta poderá ser caracterizada como falta grave, sujeitando-o às penalidades previstas na legislação e nas normas internas.

5.4 Atualização da Política

Esta política deverá ser revisada anualmente, ou sempre que ocorrerem mudanças significativas nos processos envolvidos.

6. Histórico de Revisão:

Data de alteração	Responsável	Atualização
13/12/2023	Rute Lane	Criação da Política
04/06/2025	Nathali Macedo	Revisão da Política