Política de Mesa Limpa e Tela Limpa

Proteção de informações em estações de trabalho, telas e áreas físicas da PX.Center

Código:	*POL-SEG-010*
Área responsável:	*Segurança da Informação*
Data de emissão:	*24/06/2026*
Responsável pela aprovação:	*CISO / CTO*

1. FINALIDADE/OBJETIVO

Esta política estabelece as diretrizes de mesa limpa e tela limpa da PX.Center, em conformidade com o controle 7.7 (Clear desk and clear screen) da ISO/IEC 27001:2022, com a finalidade de proteger as informações sensíveis e os ativos de informação contra acesso não autorizado, divulgação, perda ou dano decorrentes de exposição em estações de trabalho, telas, impressoras, quadros, mídias e demais áreas físicas.

O documento define as obrigações dos usuários quanto à guarda de documentos físicos, ao bloqueio de tela, ao uso de equipamentos compartilhados e ao reporte de violações, integrando os controles físicos do Sistema de Gestão de Segurança da Informação (SGSI) instituído pela POL-SEG-001.

2. ESCOPO/APLICABILIDADE

Esta política aplica-se a todos os espaços de trabalho físicos, estações de trabalho, dispositivos e mídias que permitam o acesso, o processamento, a exibição ou o armazenamento de informações corporativas da PX.Center, em todas as unidades, salas de reunião, áreas comuns e ambientes de trabalho remoto. A definição pela PX.Center como entidade de referência abrange os demais CNPJs do grupo, dispensando documento específico por entidade.

As diretrizes aplicam-se em conjunto com a POL-SEG-001 (Política de Segurança da Informação) e com a política de classificação da informação, que determina o nível de proteção exigido por cada tipo de documento ou dado.

3. USUÁRIOS/PÚBLICO-ALVO

Todos os colaboradores, estagiários, terceiros, prestadores de serviço e quaisquer pessoas que tenham acesso às instalações ou aos ativos de informação da PX.Center e que utilizem espaços de trabalho físicos ou dispositivos corporativos.

4. DOCUMENTOS DE REFERÊNCIA

- ISO/IEC 27001:2022 (controle 7.7, Clear desk and clear screen)
- Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais, LGPD)
- POL-SEG-001: Política de Segurança da Informação
- POL-SEG-013: Política de Uso Aceitável
- POL-SGI-001: Política de Ciclo de Vida da Informação
- POL-SEG-002: Política de Gestão de Incidentes

5. DIRETRIZES / REGRAS / CONTROLES

5.1 PRINCÍPIO GERAL

O usuário é responsável por proteger as informações sob sua guarda contra exposição indevida. Documentos, telas, mídias e impressões que contenham informações classificadas como internas, confidenciais ou restritas, conforme a política de classificação da informação, devem permanecer protegidos de visualização ou acesso por pessoas não autorizadas. A proteção do local de trabalho é responsabilidade conjunta da Segurança da Informação, das lideranças de cada área e do próprio usuário.

5.2 MESA LIMPA

Ao se ausentar do local de trabalho, ainda que por curtos períodos, e ao final de cada expediente, o usuário deve manter a mesa livre de documentos confidenciais e sensíveis. É obrigatório:

- Guardar documentos confidenciais e sensíveis em gavetas ou armários trancados com chave, para não ficarem visíveis ao se ausentar
- Não deixar expostos sobre a mesa contratos, planilhas, anotações, post-its, crachás ou dispositivos que contenham dados da Organização
- Recolher itens de uso pessoal que possam conter dados da empresa
- Manter a mesa limpa ao final do expediente, sem papéis soltos, dispositivos eletrônicos desprotegidos ou documentos abertos
- Descartar documentos sensíveis em fragmentadora, sendo vedado descartá-los em lixo comum.

5.3 TELA LIMPA

Ao se ausentar do computador ou dispositivo, o usuário deve impedir o acesso não autorizado à sessão ativa. É obrigatório:

- Bloquear imediatamente a tela ao se ausentar (Windows+L ou Ctrl+Alt+Del seguido de Bloquear, ou equivalente no dispositivo utilizado)
- Nunca deixar o sistema aberto ou a sessão ativa sem supervisão
- Manter o bloqueio automático de tela após período de inatividade, no padrão de 5 a 10 minutos, com retomada protegida por senha
- Não anotar senhas em locais visíveis nem deixá-las acessíveis na estação de trabalho
- Encerrar as sessões de sistemas críticos após o uso.

5.4 IMPRESSORAS E DOCUMENTOS IMPRESSOS

O usuário deve retirar imediatamente da impressora os documentos enviados para impressão, não deixando impressões esquecidas na bandeja de saída. É vedado abandonar documentos impressos em impressoras, copiadoras ou aparelhos de digitalização compartilhados. Documentos impressos por engano ou descartados devem ser eliminados em fragmentadora.

5.5 QUADROS, FLIPCHARTS E SALAS DE REUNIÃO

Ao término de reuniões, o usuário deve apagar de quadros brancos e flipcharts toda informação sensível ou confidencial e recolher anotações, materiais impressos e mídias deixados na sala. As salas de reunião devem ser conferidas antes da saída, para que nenhuma informação corporativa permaneça exposta.

5.6 DOCUMENTOS FÍSICOS E MÍDIAS

Documentos físicos e mídias que contenham informações confidenciais ou restritas devem ser armazenados em gavetas ou armários trancados com chave quando não estiverem em uso. Dispositivos de armazenamento removível, como pen drives, HDs externos e mídias de backup, devem ser guardados em local seguro e protegido, com acesso restrito por necessidade de conhecimento, sendo vedado deixá-los expostos em mesas ou áreas de circulação.

5.7 EQUIPAMENTOS E ESTAÇÕES COMPARTILHADAS

Equipamentos compartilhados, como impressoras, estações de autoatendimento, computadores de uso comum e salas de reunião, devem ser utilizados com atenção à proteção das informações. É responsabilidade do usuário verificar, ao término do uso, que nenhuma informação tenha permanecido no dispositivo, seja em documentos impressos, arquivos abertos ou sessões ativas. É vedado salvar dados confidenciais em dispositivos públicos ou compartilhados, devendo as informações ali visualizadas ser removidas imediatamente ao final do uso.

5.8 REPORTE DE VIOLAÇÃO

Toda violação a esta política, exposição indevida de informação ou suspeita de acesso não autorizado deve ser reportada imediatamente à Segurança da Informação pelo canal security@px.center. Incidentes que envolvam comprometimento de informação seguem o tratamento previsto na POL-SEG-002 (Política de Gestão de Incidentes).

6. RESPONSABILIDADES

A Tecnologia da Informação (TI), por meio da Segurança da Informação, é a área responsável por garantir o cumprimento desta política, mantém o canal security@px.center para reporte de violações e responde pela apuração de descumprimentos às suas disposições. A Direção aprova esta política e provê os recursos necessários à sua implementação, incluindo mobiliário com fechadura, fragmentadoras e configuração de bloqueio automático de tela.

As lideranças de cada área asseguram a adoção das práticas de mesa limpa e tela limpa por suas equipes e fiscalizam o cumprimento das diretrizes em seus ambientes de trabalho. Os usuários respondem pela proteção das informações sob sua guarda, observam as obrigações de mesa limpa e tela limpa, conferem equipamentos compartilhados após o uso e reportam violações pelo canal security@px.center.

7. GESTÃO DE REGISTROS

Os registros associados a esta política residem nos seguintes repositórios: - Versões desta política e evidências de divulgação: repositório documental do SGI. - Incidentes e violações reportados via security@px.center: tratados conforme a POL-SEG-002 e registrados na ferramenta corporativa de registros. - Evidências de conscientização sobre mesa limpa e tela limpa: conforme o ciclo de treinamento do SGSI. É obrigatório preservar a integridade dos registros, com acesso restrito por necessidade de conhecimento, e mantê-los disponíveis para auditorias internas e externas do SGI.

8. VALIDADE / GESTÃO DOCUMENTAL

Esta política entra em vigor em 23/06/2026, com validade por prazo indeterminado. A Segurança da Informação revisa o documento anualmente ou diante de mudança relevante nos requisitos legais ou normativos, de incidentes relacionados ao descumprimento da política ou de mudanças estruturais na Organização que impactem os controles de segurança física. O descumprimento desta política sujeita o infrator às medidas disciplinares previstas nas normas internas da PX.Center.

9. ANEXOS

Não há anexos. Os registros operacionais residem nos sistemas indicados na seção Gestão de Registros.

HISTÓRICO DE ALTERAÇÕES

Versão	Data	Criador	Descrição de Alterações
00	09/06/2025	Setor de TI e Cybersegurança - SI	Criação e Revisão
01	24/06/2026	SGI	Recodificação para sigla