POLÍTICA INTERNA DE "MESA E TELA LIMPA"

SEGURANÇA DA INFORMAÇÃO

OBJETIVO:

Esta política tem como objetivo garantir a proteção das informações confidenciais e sensíveis da cooperativa por meio de medidas de segurança relacionadas ao ambiente de trabalho, organização da mesa de trabalho e segurança das telas dos dispositivos eletrônicos. Visa reduzir o risco de acesso não autorizado, perda, furto e danos a essas informações durante e fora do horário de trabalho, alinhando-se às melhores práticas de segurança da informação e às exigências da Lei Geral de Proteção de Dados (LGPD).

Além disso, tais medidas buscam de ações que garantam:

- Tela limpa e lixo limpo, para reduzir o risco de acesso não autorizado, perda, furto e dano da informação durante e fora do horário normal de trabalho.
- Manter as áreas de trabalho organizadas e cumprindo as regras da organização.

RESPONSABILIDADES:

Todos os colaboradores são responsáveis por seguir as diretrizes estabelecidas nesta política e tomar as medidas necessárias para proteger as informações. Isso inclui a adesão aos procedimentos de mesa limpa e tela limpa e o cumprimento de medidas para proteção de dados sensíveis e confidenciais, especialmente os que dizem respeito a cooperados, clientes e processos internos.

PRATIQUE O ARMAZENAMENTO SEGURO:

É dever de todos manter o armazenamento das informações seguros, cumprindo normas e políticas, para que as informações críticas do negócio estejam sempre protegidas e guardadas em lugar seguro principalmente quando não estiverem em uso, estando ou não o escritório desocupado.

Necessário ter a devida atenção com:

- Quadros de avisos;
- Flip chart;
- Pastas e bolsa
- Listas de Tarefas
- Planejamentos

- Agendas
- Post It’s
- Documentos sobre a mesa

Esses são apenas alguns exemplos, porém é preciso atenção dentro dos costumes e ações praticadas para identificar, ações que devem ser mudadas para garantir esse armazenamento seguro.

PROCEDIMENTOS:

Cuidado em sua área de trabalho

- É importante que seu ambiente de trabalho disponha de áreas para armazenamento de documentos, como gavetas e armários com trancas, cofres ou salas de arquivo;
- Não deixe documentos em papéis e mídias removíveis, como pendrives e HDs externos, sobre sua mesa desnecessariamente;
- Atente-se para não deixar à vista anotações, recados e lembretes importantes, incluindo aqueles colados em seu monitor ou divisórias, como post-it;
- Leve seu crachá de identificação sempre com você;
- Nunca anote senhas em papéis – memorize-as ou armazene em um local seguro, como gerenciadores de senhas virtuais;
- Ao sair de uma sala de reunião, verifique se todos os papéis foram retirados, se o quadro branco foi apagado e se a folha do flipchart foi descartada apropriadamente;
- Faz parte da política de mesa limpa não fazer refeições e lanches sobre a mesa e não apoiar copos com qualquer tipo de bebida, incluindo água;
- Ao final do expediente, sempre limpe e organize sua área de trabalho.
- Lembre-se sempre: A Internet é uma ferramenta de trabalho e deve ser usada para este fim pelos funcionários, não sendo permitido o seu uso para fins recreativos e pessoais durante o horário de trabalho;
- É obrigatória a manutenção da caixa de e-mail, evitando acúmulo de e-mails e arquivos inúteis – Organize-se Profissionalmente;
- Se a impressão de algum documento apresentar problema e o papel puder ser reaproveitado na sua próxima tentativa, sem comprometer as informações, recolocá-lo na bandeja de impressão.
- Caso contrário, se o papel servir para rascunho, o usuário deverá levá-lo para sua mesa. Se o papel não puder ser reaproveitado por conter diversas informações confidenciais, deve ser picotado, de forma mecânica ou manual, e colocado no lixo de forma segura, quando não houver picotadora de papel disponível.

Informações sensíveis e confidenciais merecem atenção especial

- Documentos com Informações estratégicas, internas ou de cooperados, devem ser devidamente guardados em gavetas ou armários trancados quando não estiverem em uso e ao final do dia;
- Mantenha agendas, cadernos e pertences pessoais em gavetas fechadas;
- Materiais muito importantes ou confidenciais devem ser trancados em um local à prova de fogo, como cofres, para que sejam facilmente recuperados em caso de incêndio ou evacuação;
- Documentos impressos que contenham informações sensíveis devem ser destruídos completamente, de preferência em fragmentadoras, antes de serem descartados;
- Evite que papéis sobre a mesa sejam visíveis de janelas ou corredores;
- Se você manuseia informações sensíveis, posicione seu monitor ou notebook de forma a evitar que pessoas possam olhar sua tela e utilize película ou filtro de privacidade.

Cautela ao usar impressoras e copiadoras

- Adote uma cultura sem papel: não imprima documentos de forma desnecessária, apenas para leitura. Prefira ler na tela do computador, tablet ou celular sempre que possível;
- Ao imprimir informações sensíveis ou confidenciais, retire-as da impressora imediatamente;
- Avalie instalar impressoras com funções de senha ou ativadas por crachá, por exemplo, para que o documento impresso seja liberado apenas para o requerente da impressão;
- Bloqueie impressoras, copiadoras e scanners após o horário do expediente;
- Reduza a quantidade de papel configurando a impressão para frente e verso.

Proteção de dispositivos e sistemas

- Da mesma forma que sua mesa, procure manter a área de trabalho do seu computador limpa e organizada, com os arquivos guardados em pastas, devidamente identificados e com backup seguro e constante;
- Evite manter os arquivos localmente no computador – prefira sempre armazenar os dados em local indicado pela área de segurança;
- Computadores pessoais e impressoras não devem ser deixados “logados” quando não houver usuário junto e devem estar protegidos por senhas e outros controles quando não estiverem sendo utilizados;
- Configure seu computador para bloquear automaticamente e acionar o protetor de tela após 2 ou 3 minutos de ociosidade, com desbloqueio apenas por senha;
- Mesmo com a configuração, é recomendado que bloqueie o computador manualmente sempre que levantar da mesa;

- Ao final do dia, desligue o computador, principalmente aqueles que estão em rede, e verifique se não há nenhuma mídia removível conectada nele.
- **Backup Seguro**: Certifique-se de que todos os dados importantes estejam armazenados de forma segura em sistemas indicados pela área de TI, evitando armazenar arquivos localmente no computador.

CUIDADOS COM O LIXO:

Muitas informações são descartadas sem os devidos cuidados, dando acesso a quem não deveria ter, principalmente quando se fala em documento físico. O lixo é uma fonte de informação sobre a pessoa que a produz, em uma empresa onde são reunidos vários documentos de vários departamentos é preciso ter muito cuidado com a forma que será realizado o descarte.

Desta forma, deve adotar o processo onde todo lixo que contenha informação reservada ou secreta deve ser eliminado através de "Máquina picotadora" ou similar, ou destruição manual.

Sempre se certifique que o descarte ocorreu de maneira correta e que impossibilita qualquer tentativa de reconstrução.

É preciso tomar alguns cuidados como verificar sempre o que está na sua "lata de lixo", afinal muitos curiosos gostam de saber o que você está jogando fora.

TELETRABALHO E SEGURANÇA REMOTA

- No caso de trabalho remoto, utilize VPN para acessar os sistemas da cooperativa e proteja os dispositivos com senhas fortes e criptografia.
- Evitar o uso de dispositivos pessoais sem a devida segurança (ex.: antivírus, firewalls).
- Nunca utilize redes públicas sem segurança para acessar informações da cooperativa.

CONSCIENTIZAÇÃO E TREINAMENTO:

- A cooperativa promoverá treinamentos regulares sobre segurança da informação, focando nas práticas de mesa e tela limpa, manuseio e descarte de informações sensíveis, além de diretrizes específicas da LGPD.
- Esses treinamentos serão obrigatórios para todos os colaboradores e realizados ao menos anualmente.

MONITORAMENTO E FISCALIZAÇÃO:

- A área de segurança da informação realizará auditorias semestrais para verificar o cumprimento desta política e aplicar medidas corretivas em caso de não conformidade.

- Indicadores de conformidade serão estabelecidos, como o número de incidentes reportados e o percentual de colaboradores treinados, para medir a eficácia da política.

CANAL DE DENÚNCIAS E DÚVIDAS

- Os colaboradores que tenham dúvidas ou preocupações sobre a aplicação desta política ou que desejem reportar incidentes de segurança podem utilizar o canal de denúncias confidencial, disponível por meio de e-mail específico e ferramentas de reporte anônimas.
- Denúncias serão tratadas com confidencialidade, conforme as exigências da LGPD, e investigadas de maneira imparcial.

SANÇÕES

A não conformidade com esta política sujeitará o colaborador a sanções administrativas e, em casos graves, a possíveis ações legais, conforme previsto nas normas internas da cooperativa e legislação aplicável.

REVISÃO E ATUALIZAÇÃO

Esta política será revisada **anualmente** e poderá ser atualizada de acordo com mudanças nas práticas de segurança da informação ou alterações na legislação, incluindo as regulamentações da LGPD.

DISPOSIÇÕES GERAIS:

Esta política entra em vigor a partir da data de sua aprovação e deverá ser revisada periodicamente para garantir sua eficácia e atualização de acordo com as mudanças nas práticas de segurança da informação.

Data de aprovação: 27/09/2024