

DOCUMENTO INSTITUCIONAL

Política de Segurança da Informação

Summo Quartile

APLICA-SE A

sócios, empregados, prestadores de serviço e terceiros autorizados a acessar informações ou ambientes da Summo Quartile anual ou quando houver mudança material no ambiente operacional, tecnológico ou regulatório

1. Objetivo

Esta Política estabelece os controles mínimos para proteger a confidencialidade, a integridade, a disponibilidade e a rastreabilidade das informações sob responsabilidade da Summo Quartile. A empresa atua com documentos técnicos, comerciais, contratuais e estratégicos ligados a relações institucionais sensíveis e, por isso, exige disciplina informacional compatível com a criticidade dos dados tratados. Define regras para o uso, o armazenamento, o compartilhamento, a proteção e o descarte de informações e documentos da empresa e de seus clientes, parceiros e interlocutores.

2. Aplicabilidade

Esta Política aplica-se a:

- sócios e dirigentes;
- empregados, estagiários e colaboradores eventuais;
- consultores, representantes e prestadores de serviço;
- terceiros autorizados a acessar informações ou ambientes da Summo Quartile;
- documentos físicos e digitais sob guarda da empresa.

3. Princípios de segurança

As informações da Summo Quartile devem ser tratadas conforme os seguintes princípios:

- Confidencialidade — acesso apenas por quem precisa conhecer;
- Integridade — preservação da exatidão e da consistência;
- Disponibilidade — acesso adequado quando necessário;
- Rastreabilidade — possibilidade de identificar uso, versões e fluxos relevantes;
- Proporcionalidade — controles compatíveis com o nível de sensibilidade.

4. Classificação da informação

As informações devem ser classificadas de forma simples e objetiva:

CLASSE	USO ESPERADO
Pública	Pode ser divulgada sem risco relevante
Interna	Uso restrito ao ambiente de trabalho da Summo Quartile
Confidencial	Acesso controlado, com impacto relevante em caso de divulgação indevida
Restrita	Acesso limitado e controle reforçado

Documentos de cliente, dados pessoais, oportunidades não públicas, contratos, estudos técnicos e ambientes de projeto devem ser tratados, como regra, no mínimo como confidenciais.

5. Controle de acesso

O acesso a informações e sistemas deve seguir o princípio do menor privilégio. Isso significa que:

- cada pessoa recebe apenas o acesso necessário ao seu papel;
- credenciais são pessoais e intransferíveis;
- acessos devem ser revistos quando houver mudança de função, projeto ou desligamento;
- informações restritas exigem controle reforçado.

Os responsáveis por ambiente, pasta, sistema ou projeto devem zelar pela coerência entre os acessos concedidos e a necessidade funcional efetiva.

6. Compartilhamento interno e externo

Toda circulação de informação deve observar necessidade, adequação e canal apropriado. Não é permitido:

- compartilhar documentos confidenciais sem base funcional;
- enviar arquivos sensíveis por canais inadequados;
- armazenar documentos relevantes em ambientes não autorizados;
- utilizar endereços de acesso público para documentos com dados pessoais ou confidenciais;
- manter cópias desnecessárias de informações restritas.

Sempre que houver compartilhamento externo de informação confidencial ou restrita, deve haver base funcional legítima, controle mínimo de destinatários e preferência por ambientes com permissão gerenciável.

7. Ambientes de cliente e documentos restritos

Documentos de cliente e ambientes restritos devem, sempre que possível, observar:

- autenticação reforçada;
- controle de permissão por usuário ou projeto;
- registro de versões;
- trilha de auditoria para acessos relevantes;
- expiração ou revisão periódica de acessos.

O armazenamento de informações da Summo Quartile deve ocorrer em plataformas com certificações de segurança reconhecidas (por exemplo, Google Drive e Microsoft 365).

8. Senhas, MFA e dispositivos

Todos devem adotar cuidados mínimos com credenciais e equipamentos utilizados em atividades da Summo Quartile:

- senhas fortes e não compartilhadas;
- ativação de MFA (autenticação em dois fatores) quando disponível, especialmente em ferramentas que armazenam dados pessoais;
- bloqueio de tela e proteção básica dos dispositivos;
- uso responsável de equipamentos pessoais em contexto profissional.

Em acessos remotos, redes compartilhadas ou uso de equipamento pessoal, o usuário deve adotar cautela reforçada para evitar visualização indevida, captura não autorizada ou permanência de arquivos fora de ambiente controlado.

9. Cópia de segurança, retenção e descarte

Informações relevantes devem seguir critério razoável de retenção, recuperação e descarte. Sempre que aplicável:

- documentos ativos devem permanecer em ambiente controlado;
- arquivos obsoletos ou duplicados devem ser eliminados de forma segura;
- materiais sensíveis não devem permanecer indefinidamente sem necessidade;
- o descarte deve considerar a classificação da informação e os prazos de retenção previstos na Política de Privacidade e Proteção de Dados.

10. Incidentes de segurança

Incidentes ou suspeitas de incidente devem ser reportados imediatamente. Exemplos:

- envio indevido de documento;
- acesso não autorizado;
- perda de dispositivo com informações da Summo Quartile;
- vazamento ou suspeita de vazamento;
- alteração indevida de arquivo relevante.

Toda ocorrência deve ser registrada e tratada de forma proporcional à criticidade do caso, contemplando contenção inicial, preservação de evidências, avaliação de impacto, comunicação aos responsáveis e definição de medidas de correção. Quando o incidente envolver dados pessoais e puder acarretar risco aos titulares, observa-se também a notificação à ANPD nos termos da LGPD.

11. Responsabilidades dos usuários

Toda pessoa com acesso a informações da Summo Quartile deve:

- observar a classificação aplicável ao documento ou ambiente;
- manter organização mínima de pastas, versões e nomenclaturas;
- reportar acessos indevidos, fragilidades percebidas ou dúvidas relevantes;
- encerrar ou devolver acessos, arquivos e materiais quando cessar a necessidade de uso.

12. Treinamento e responsabilização

As pessoas sujeitas a esta Política devem receber orientação adequada sobre o tratamento das informações em seu contexto de trabalho. O descumprimento das regras pode gerar medida corretiva, restritiva, disciplinar ou contratual, conforme a gravidade do caso.

Esta Política integra o conjunto de governança da Summo Quartile e deve ser lida em conjunto com o Código de Ética e Conduta e a Política de Privacidade e Proteção de Dados.