Política Institucional		
Área Gestora **Compliance e Gestão de Riscos**	Código 0001	Versão 002
Assunto **Política de Segurança da Informação**	Data de Criação 04/11/2026	Data de Publicação 06/11/2026
Abrangência **Limitada à Arton Capital**		

Política de Segurança da Informação — Arton Capital

1. OBJETIVO E ABRANGÊNCIA

A presente Política de Segurança da Informação ("Política") estabelece os princípios, regras e procedimentos adotados pela Arton Capital, estruturada através da Panah Participações Ltda., para a proteção das informações relacionadas ao exercício da atividade de coordenação de ofertas públicas de valores mobiliários, incluindo a verificação periódica dos controles de segurança e a identificação dos detentores de informações confidenciais.

Esta Política aplica-se a todos os sócios, diretores, empregados, estagiários e demais colaboradores da Arton Capital, incluindo os Profissionais Compartilhados alocados às suas atividades (em conjunto, "Colaboradores" e, individualmente, "Colaborador"), bem como, no que couber, à empresa prestadora de serviço terceirizado de tecnologia da informação ("Prestadora de TI"), no suporte técnico prestado à Arton Capital.

Os termos iniciados em letra maiúscula não definidos nesta Política têm o significado que lhes é atribuído no Manual de Segregação de Atividades e Confidencialidade da Arton Capital ("Manual de Segregação").

Esta Política foi elaborada de forma proporcional ao porte e à estrutura da Arton Capital, cuja estrutura alocada é composta por 6 (seis) profissionais, relacionados no item 3.2 do Manual de Segregação, e cujas informações são mantidas em ambiente de nuvem, nos termos da seção 3.

2. PRINCÍPIOS

A proteção das informações da Arton Capital observa os seguintes princípios:

• confidencialidade: as informações somente devem ser acessadas por pessoas autorizadas e utilizadas para as finalidades profissionais que justificaram o acesso;

• integridade: as informações devem ser preservadas contra alteração ou exclusão não autorizada, mantendo-se sua exatidão e completude;

• disponibilidade: as informações devem estar acessíveis aos Colaboradores autorizados sempre que necessárias ao exercício de suas funções; e

• necessidade de acesso: o acesso a informações e a recursos tecnológicos é concedido na medida necessária ao exercício das funções de cada Colaborador.

3. AMBIENTE TECNOLÓGICO E ARMAZENAMENTO DAS INFORMAÇÕES

A Arton Capital utiliza o Microsoft 365 (Office 365), incluindo e-mail corporativo, e mantém as informações e os documentos relativos às suas atividades na Pasta Eletrônica da Arton Capital, em ambiente de nuvem, por meio do OneDrive. A infraestrutura tecnológica é disponibilizada no

âmbito do Grupo Arton, em regime de Compartilhamento Controlado, nos termos dos itens 8.1 e 9.2 do Manual de Segregação.

As informações e os documentos relativos às ofertas públicas e às demais atividades da Arton Capital devem ser armazenados na Pasta Eletrônica da Arton Capital. É vedado aos Colaboradores armazenar Informações Confidenciais da Arton Capital em pastas, diretórios ou repositórios de outras sociedades do Grupo Arton, bem como em dispositivos ou contas pessoais.

As atas, os registros e os documentos relacionados ao Comitê de Aceitação de Operações são armazenados em diretório eletrônico segregado, com acesso controlado.

Os equipamentos utilizados pelos Colaboradores são de uso individual e não são compartilhados entre profissionais, nos termos do item 9.1 do Manual de Segregação.

4. GESTÃO DE ACESSOS

4.1. Regra geral

O acesso permanente à Pasta Eletrônica da Arton Capital é restrito aos 6 (seis) profissionais indicados no item 3.2 do Manual de Segregação. Os profissionais de outras sociedades do Grupo Arton não possuem acesso funcional permanente à Pasta Eletrônica da Arton Capital, e a disponibilização da infraestrutura tecnológica pelo Grupo Arton não lhes confere esse acesso.

4.2. Concessão e alteração de acessos

A concessão de novos acessos e a alteração de acessos existentes dependem de aprovação prévia, conforme a governança interna aplicável, e são executadas tecnicamente pela Prestadora de TI, observados a necessidade funcional e o princípio da necessidade de acesso.

4.3. Movimentação de Colaboradores

Sempre que um Colaborador tiver suas funções alteradas, seus acessos deverão ser ajustados às novas funções, mediante aprovação prévia e execução técnica pela Prestadora de TI, na forma do item 4.2. O Colaborador que deixar de estar alocado às atividades da Arton Capital terá seus acessos à Pasta Eletrônica da Arton Capital revogados.

4.4. Desligamentos

No desligamento de Colaborador, seus acessos à Pasta Eletrônica da Arton Capital e aos demais recursos tecnológicos utilizados nas atividades da Arton Capital deverão ser revogados. O Colaborador desligado permanece obrigado a observar os deveres de confidencialidade e sigilo previstos no Manual de Segregação e no Código de Ética.

4.5. Revisão periódica

Os acessos existentes serão revisados periodicamente, no âmbito da verificação prevista na seção 10.

4.6. Credenciais

As credenciais de acesso ao Microsoft 365 e aos demais recursos tecnológicos são pessoais e intransferíveis, sendo vedado seu compartilhamento.

5. ACESSO REMOTO

O ambiente em nuvem permite que os Colaboradores autorizados acessem remotamente as informações da Arton Capital, inclusive fora do escritório. O acesso remoto observa as mesmas regras de acesso, armazenamento e confidencialidade previstas nesta Política e no Manual de Segregação e somente pode ser realizado mediante as credenciais pessoais do Colaborador.

No acesso remoto, o Colaborador deverá adotar cautelas compatíveis com a confidencialidade das informações, evitando ambientes e situações que permitam sua visualização ou obtenção por terceiros.

6. INFORMAÇÕES CONFIDENCIAIS E DOCUMENTOS DE OFERTAS PÚBLICAS

As Informações Confidenciais e as Informações Relevantes e Não Públicas, incluindo a documentação relativa às ofertas públicas, observam as regras de confidencialidade, circulação restrita e necessidade funcional previstas no Manual de Segregação e no Código de Ética, destacando-se que:

• a documentação das ofertas é armazenada na Pasta Eletrônica da Arton Capital, nos termos da seção 3;

• o encaminhamento de Informações Confidenciais por e-mail deve limitar-se aos destinatários com necessidade funcional;

• o compartilhamento de arquivos da Pasta Eletrônica da Arton Capital com pessoas externas à Arton Capital, inclusive profissionais de outras sociedades do Grupo Arton, somente poderá ocorrer nas hipóteses do item 11.3 do Manual de Segregação, limitado aos documentos estritamente necessários; e

• é vedada a retirada ou a cópia de Informações Confidenciais para ambientes externos à Arton Capital, salvo quando necessária ao exercício das funções do Colaborador e compatível com o Manual de Segregação.

6.1. Identificação dos detentores das informações

A identificação das pessoas que detêm Informações Confidenciais e Informações Relevantes e Não Públicas, inclusive para fins de responsabilização em caso de vazamento, é realizada:

• em caráter permanente, pela relação dos profissionais com acesso à Pasta Eletrônica da Arton Capital, correspondente aos 6 (seis) profissionais indicados no item 3.2 do Manual de Segregação;

• em relação a cada oferta, pelo controle de Pessoas com Acesso mantido pela Estrutura de Compliance, nos termos do item 13 do Manual de Segregação; e

• quando necessário, pelos registros de acesso e de atividade disponibilizados pela infraestrutura tecnológica utilizada, nos termos da seção 8.

7. INCIDENTES DE SEGURANÇA

Considera-se incidente de segurança qualquer evento, confirmado ou suspeito, que comprometa ou possa comprometer a confidencialidade, a integridade ou a disponibilidade das informações da Arton Capital, tais como acesso indevido, vazamento de informações, perda ou furto de equipamento, comprometimento de credenciais ou exclusão indevida de informações.

Os incidentes de segurança serão tratados da seguinte forma:

• identificação e comunicação: o Colaborador que identificar incidente ou suspeita de incidente deverá comunicá-lo imediatamente ao Diretor de Compliance;

• análise: a Estrutura de Compliance, com o apoio técnico da Prestadora de TI quando necessário, avaliará a natureza e a extensão do incidente, as informações afetadas e as pessoas envolvidas, podendo utilizar o controle de Pessoas com Acesso e os registros disponíveis nos termos da seção 8;

• medidas corretivas: serão adotadas as medidas cabíveis, tais como a alteração de credenciais, o ajuste ou a revogação de acessos, a recuperação das informações na medida dos recursos disponíveis, a aplicação das medidas previstas no Manual de Compliance e no Manual de Segregação e, conforme o caso, as comunicações exigidas pela legislação e pela regulamentação aplicáveis; e

• registro: quando aplicável, o incidente, a análise realizada e as medidas adotadas serão registrados e arquivados eletronicamente pela Estrutura de Compliance.

8. REGISTROS DE ACESSO E RASTREABILIDADE

Para fins de rastreabilidade, a Arton Capital utiliza os controles de acesso e os registros de acesso e de atividade disponibilizados pelas funcionalidades da infraestrutura tecnológica utilizada, na extensão em que disponíveis.

Esses registros poderão ser obtidos com o auxílio da Prestadora de TI quando necessários à verificação periódica prevista na seção 10 ou à investigação de incidente de segurança.

9. CONTINUIDADE E RECUPERAÇÃO DAS INFORMAÇÕES

A manutenção das informações em ambiente de nuvem permite que os Colaboradores autorizados acessem remotamente as informações da Arton Capital, inclusive em caso de indisponibilidade das instalações físicas ou de equipamento individual, preservando a continuidade das atividades.

A recuperação de informações eventualmente excluídas, alteradas ou indisponíveis será conduzida com o apoio técnico da Prestadora de TI, na medida dos recursos disponibilizados pelo ambiente tecnológico utilizado, observados os prazos de guarda documental previstos no Manual de Compliance.

9.1. Backup e recuperação de informações

Sem prejuízo dos mecanismos de armazenamento e recuperação disponibilizados pelo ambiente Microsoft 365, a Arton Capital mantém solução adicional de backup em nuvem contratada para as contas dos 4 (quatro) profissionais integrantes de sua equipe de intermediação que atuam diariamente na produção e manutenção da documentação operacional da Arton Capital.

A solução de backup contempla o ambiente Microsoft 365 utilizado por esses profissionais, incluindo e-mails, OneDrive, SharePoint e Teams, com retenção de dados de até 7 (sete) anos.

A Prestadora de TI é responsável pelo suporte técnico relacionado à solução contratada e, quando necessário, pelo apoio aos procedimentos de recuperação das informações, observadas as funcionalidades e condições disponibilizadas pelo prestador do serviço.

A existência da solução adicional de backup não altera as regras de controle de acesso às informações da Arton Capital previstas nesta Política, permanecendo o acesso às informações restrito aos profissionais autorizados, de acordo com suas respectivas funções e atribuições.

10. TESTES E VERIFICAÇÕES PERIÓDICAS DE SEGURANÇA

A Estrutura de Compliance, com o apoio técnico da Prestadora de TI, realizará verificação dos controles de segurança da informação com periodicidade anual e, extraordinariamente, sempre que ocorrer incidente de segurança relevante ou alteração relevante na estrutura de profissionais ou no ambiente tecnológico da Arton Capital.

A verificação contemplará, conforme aplicável:

• a revisão dos usuários com acesso à Pasta Eletrônica da Arton Capital;

• a confirmação de que os acessos existentes continuam compatíveis com as funções exercidas pelos respectivos Colaboradores;

• a verificação de que as concessões, alterações e revogações de acessos decorrentes de admissões, desligamentos e alterações de função foram realizadas;

• a verificação de eventuais acessos indevidos ou incompatíveis com esta Política;

• a análise dos registros de acesso e de atividade disponíveis, quando necessária para a investigação de incidente de segurança; e

• o registro das verificações realizadas e das medidas corretivas eventualmente adotadas.

Cada verificação será documentada em registro que indique a data, os responsáveis, o escopo, o resultado, as inconsistências identificadas e as medidas corretivas adotadas, o qual será arquivado eletronicamente pela Estrutura de Compliance.

Identificado acesso indevido ou incompatível, a Estrutura de Compliance solicitará à Prestadora de TI o ajuste ou a revogação do acesso e, se a situação indicar incidente de segurança, adotará os procedimentos da seção 7.

11. RESPONSABILIDADES

11.1. Compliance

Compete ao Diretor de Compliance, com o apoio da Estrutura de Compliance:

• implementar esta Política e acompanhar a aderência a ela;

• conduzir as verificações periódicas de acessos e controles previstas na seção 10;

• receber as comunicações de incidentes e acompanhar os incidentes relevantes sob a perspectiva de Compliance e de confidencialidade; e

• revisar esta Política, nos termos da seção 13.

11.2. Prestadora de TI

Compete à Prestadora de TI, no suporte prestado à Arton Capital:

• executar tecnicamente as concessões, alterações e revogações de acessos autorizadas;

• prestar suporte à infraestrutura tecnológica utilizada pela Arton Capital; e

• auxiliar, quando necessário, na obtenção de registros e de informações técnicas disponíveis, inclusive para as verificações periódicas e a investigação de incidentes.

11.3. Colaboradores

Compete aos Colaboradores:

• preservar suas credenciais de acesso, que são pessoais e intransferíveis;

• respeitar as limitações de acesso aplicáveis;

• utilizar os sistemas e as informações exclusivamente para as finalidades profissionais autorizadas; e

• comunicar imediatamente ao Diretor de Compliance incidentes ou suspeitas de incidentes de segurança.

12. TREINAMENTO, CIÊNCIA E VIOLAÇÕES

Esta Política integra o programa de treinamento previsto no Manual de Compliance, e os Colaboradores deverão confirmar sua leitura, entendimento e cumprimento mediante o Termo de Adesão previsto no Manual de Compliance.

O descumprimento desta Política sujeita o Colaborador às medidas previstas no Manual de Compliance e no Manual de Segregação, sem prejuízo das demais medidas cabíveis.

13. REVISÃO DA POLÍTICA

O Diretor de Compliance revisará esta Política pelo menos anualmente e, a qualquer tempo, sempre que houver alteração regulatória, operacional ou institucional relevante, incluindo alteração do ambiente tecnológico, da estrutura de profissionais ou das estruturas compartilhadas, bem como quando a verificação periódica ou a análise de incidente indicar a necessidade de ajuste.

Esta Política constitui documento institucional da Arton Capital e deverá ser interpretada em conjunto com o Manual de Compliance, o Código de Ética, o Manual de Segregação, a Política de PLD e Cadastro e a Política de Investimentos em Valores Mobiliários da Arton Capital, observada a legislação aplicável à proteção de dados pessoais.