Herdade
CAPITAL

Política de Segurança da Informação

e Segurança Cibernética

Versão 1.1

Agosto de 2026

Aprovada pela reunião de sócios

Documento público, disponível em herdadecapital.com.br

1. OBJETIVO E ABRANGÊNCIA

1.1. Esta Política estabelece as regras adotadas pela HERDADE CAPITAL LTDA., inscrita no CNPJ/MF sob o nº 59.969.008/0001-03 (a "Sociedade"), para proteger a confidencialidade, a integridade e a disponibilidade das informações sob sua responsabilidade, em especial as informações de clientes obtidas no exercício da atividade de consultoria de valores mobiliários.

1.2. Aplica-se a todos os sócios, diretores, empregados, estagiários e prestadores de serviços com acesso a informações ou sistemas da Sociedade (os "Colaboradores"), em qualquer local de trabalho, inclusive em regime remoto, e observa a Resolução CVM nº 19/2021, quanto ao dever de sigilo e aos controles internos, e a Lei nº 13.709/2018.

1.3. Os Colaboradores aderem a esta Política mediante assinatura do Termo constante do Anexo I.

2. RESPONSABILIDADES

2.1. O Diretor de Compliance é responsável por implementar e fiscalizar esta Política, autorizar a concessão e a revogação de acessos, aprovar os programas utilizados e coordenar o tratamento de incidentes.

2.2. A infraestrutura de tecnologia é administrada por prestador especializado contratado, responsável pela operação de firewall e rede, pela gestão de contas e licenças, pela administração do antivírus e pela execução das rotinas de backup, sob supervisão do Diretor de Compliance e mediante contrato que contenha obrigações de confidencialidade e de comunicação imediata de incidentes.

2.3. Cada Colaborador responde pela guarda das credenciais que lhe forem atribuídas, pelo uso adequado dos recursos e pela comunicação imediata de qualquer suspeita de incidente, perda de dispositivo ou acesso não autorizado.

3. CONFIDENCIALIDADE E CONTROLE DE ACESSO

3.1. São confidenciais os dados cadastrais, patrimoniais e financeiros de clientes, as recomendações de investimento, os contratos, os dados pessoais de Colaboradores e as credenciais de acesso. Essas informações são acessadas apenas por quem delas necessite para o desempenho de suas atividades e armazenadas exclusivamente em repositórios corporativos.

3.2. O acesso a sistemas e arquivos é concedido mediante credenciais individuais e intransferíveis, autorizadas pelo Diretor de Compliance. As senhas obedecem a requisitos mínimos de complexidade, não são compartilhadas e são acompanhadas de autenticação em dois fatores no correio eletrônico corporativo e nos serviços em nuvem, sempre que a funcionalidade estiver disponível.

3.3. As estações de trabalho e os dispositivos móveis corporativos bloqueiam automaticamente após período de inatividade.

3.4. Em caso de desligamento, afastamento prolongado ou mudança de função, os acessos são bloqueados ou revogados imediatamente, inclusive em sistemas de terceiros.

4. USO DOS RECURSOS DE TECNOLOGIA

4.1. Os equipamentos, o correio eletrônico e os demais recursos disponibilizados destinam-se ao exercício das atividades profissionais e podem ser monitorados pela Sociedade para verificação de conformidade com esta Política, observada a legislação aplicável.

4.2. Somente podem ser instalados programas previamente autorizados pelo Diretor de Compliance e regularmente licenciados.

4.3. É vedado o armazenamento de informação confidencial em dispositivos pessoais, em serviços de nuvem não corporativos ou em mídias removíveis não autorizadas.

4.4. Ferramentas de inteligência artificial generativa somente podem ser utilizadas em versões corporativas homologadas pelo Diretor de Compliance, sendo vedada a inserção de dados de clientes ou de qualquer informação confidencial em ferramentas públicas ou gratuitas.

4.5. Documentos impressos que contenham informação confidencial são retirados imediatamente da impressora, não são mantidos sobre mesas desocupadas e são fragmentados após o uso. Mídias eletrônicas descartadas são apagadas de modo que a informação não possa ser recuperada.

5. BACKUP E CONTINUIDADE

5.1. Os arquivos corporativos são objeto de backup diário em nuvem, executado pelo prestador de tecnologia, com retenção compatível com o prazo regulatório de guarda de 5 (cinco) anos.

5.2. A rede é protegida por firewall e as estações de trabalho contam com antivírus atualizado. Os sistemas operacionais e aplicativos são mantidos atualizados pelo prestador de tecnologia.

5.3. Na hipótese de indisponibilidade das instalações físicas ou da rede local, as atividades prosseguem em regime remoto, com acesso aos arquivos e sistemas mantidos em nuvem.

6. INCIDENTES DE SEGURANÇA

6.1. Considera-se incidente qualquer evento, confirmado ou suspeito, que possa comprometer a confidencialidade, a integridade ou a disponibilidade das informações, incluindo acesso não autorizado, vazamento, perda de dispositivo, indisponibilidade de sistemas e infecção por código malicioso.

6.2. O Colaborador que identificar ou suspeitar de incidente comunica imediatamente o Diretor de Compliance, que aciona o prestador de tecnologia e adota as medidas de contenção cabíveis, tais como bloqueio de credenciais, isolamento de equipamentos e restauração de backup.

6.3. O incidente é registrado com a data, a descrição do evento, as informações afetadas, as medidas adotadas e as providências de prevenção, e o registro é arquivado pelo prazo de 5 (cinco) anos.

6.4. Havendo comprometimento de informações de clientes, o Diretor de Compliance comunica os titulares afetados e avalia a comunicação à Autoridade Nacional de Proteção de Dados, nos termos do art. 48 da Lei nº 13.709/2018, e à CVM, quando o evento for relevante para a regularidade das atividades.

7. DISPOSIÇÕES FINAIS

7.1. Os contratos com prestadores que tenham acesso a informações da Sociedade ou de seus clientes contêm obrigações de confidencialidade, requisitos mínimos de segurança, vedação de uso para finalidade diversa e obrigação de comunicação imediata de incidentes.

7.2. O descumprimento desta Política caracteriza falta grave e sujeita o Colaborador a advertência, suspensão, desligamento por justa causa ou exclusão do quadro societário, sem prejuízo das responsabilidades civil, administrativa e penal aplicáveis.

7.3. Esta Política entra em vigor na data de sua aprovação, prevalece sobre entendimentos anteriores e é revisada, no mínimo, a cada 2 (dois) anos ou diante de alteração relevante na estrutura tecnológica, mantido o controle de versões pelo Diretor de Compliance.

São Paulo, [dia] de [mês] de 2026.

Diretoria de Compliance

ANEXO I. TERMO DE ADESÃO

Pelo presente instrumento, [nome completo], inscrito(a) no CPF/MF sob o nº [.....], na qualidade de [cargo] da HERDADE CAPITAL LTDA., sociedade inscrita no CNPJ/MF sob o nº 59.969.008/0001-03, com sede na cidade de São Paulo, Estado de São Paulo, declara ter recebido, lido e compreendido a Política de Segurança da Informação e Segurança Cibernética da Herdade Capital, obrigando-se a observá-la integralmente.

Obriga-se a utilizar os recursos de tecnologia exclusivamente para fins profissionais, a preservar o sigilo das informações a que tiver acesso e a comunicar imediatamente qualquer incidente ou suspeita de incidente, e declara estar ciente de que os recursos corporativos podem ser monitorados pela Sociedade.

Declara, ainda, ter ciência de que o descumprimento caracteriza falta grave, sujeitando-o às penalidades internas cabíveis, sem prejuízo das responsabilidades civil, administrativa e penal.

São Paulo, [dia] de [mês] de 20[..].

_____

[Nome completo]
CPF/MF nº [.....]