FUNDAÇÃO DE ENSINO
SUPERIOR DO VALE DO SAPUCAÍ

Política de
Gestão das Informações da Organização, Privacidade e Proteção de Dados

CONSELHO DIRETOR

Portaria 007/2025

Institui a POLÍTICA DE GESTÃO DAS INFORMAÇÕES DA ORGANIZAÇÃO, PRIVACIDADE E PROTEÇÃO DE DADOS da Fundação de Ensino Superior do Vale do Sapucaí e de suas Mantidas.

O Conselho Diretor da Fundação de Ensino Superior do Vale do Sapucaí – FUVS, representado neste ato pelos seus conselheiros, no uso das atribuições que lhe confere o inciso "XII" do art. 22, de seu Estatuto, aprovado pelo Conselho Deliberativo em 25 de março de 2024, e

Considerando que a missão da FUVS é "promover o desenvolvimento das pessoas por intermédio de suas Mantidas, oferecendo soluções qualificadas em educação e saúde".

Considerando que a visão da FUVS é "consolidar-se como gestora eficiente e eficaz de recursos, que contribui para o cumprimento das missões, visões e demais objetivos de suas Mantidas".

Considerando que os valores institucionais são: **Segurança** – Cuidado e responsabilidade em todos os atos e processos; **Profissionalismo** – Foco na entrega das melhores soluções viáveis; **Empatia** – Compreensão verdadeira das necessidades das pessoas; **Resultado sustentável** – Fundamental para a perenidade institucional; e **Responsabilidade social** – Atuação com respeito às questões ambientais, sociais e à governança íntegra, ética e transparente.

Considerando a importância de fortalecer a imagem institucional da FUVS e suas Mantidas perante a sociedade e públicos de seu interesse *(stakeholders)*.

Considerando a necessidade de padronizar e orientar a interação entre a FUVS e suas Mantidas com seus públicos de interesse, sejam eles clientes, usuários, funcionários, fornecedores, prestadores de serviços e, ainda, entes públicos.

Considerando o conceito de Gestão da Informação como sendo o conjunto de práticas utilizadas para coletar, armazenar, organizar e utilizar os dados que circulam pela instituição.

Considerando que esses dados podem gerar, em sua maioria, negócios para a FUVS e suas Mantidas, sendo estratégico seu uso.

Considerando os riscos existentes caso não haja um rígido controle sobre esses dados, inclusive pela obrigatoriedade de se cumprir a Lei Geral de Proteção de Dados (LGPD).

Considerando a importância de instituir uma Política de Gestão das Informações da Organização, Privacidade e Proteção de Dados que auxilie no trabalho profissional e eficaz por parte dos funcionários, que contribua para a melhoria dos processos e possa maximizar o desempenho da FUVS e de suas Mantidas, respeitando a legalidade dos atos.

Considerando que o conteúdo desta política foi aprovado em reunião ordinária do **Conselho Deliberativo** da FUVS, em 28/04/2025, ata 02/2025, **RESOLVE**:

Art. 1º. Fica instituída a POLÍTICA DE GESTÃO DAS INFORMAÇÕES DA ORGANIZAÇÃO, PRIVACIDADE E PROTEÇÃO DE DADOS da FUVS e de suas Mantidas, nos termos dos capítulos e artigos descritos a seguir:

Capítulo I
DOS PRINCÍPIOS NORTEADORES

Art. 2º. A FUVS e suas Mantidas têm por princípio respeitar a privacidade e segurança dos dados das pessoas a que têm acesso e procura, em seus processos estabelecidos, se certificar de que o tratamento dos dados pessoais ocorra de forma transparente, não sendo realizado para finalidades distintas ou incompatíveis àquelas que fundamentam sua coleta.

Parágrafo único. Todos os trabalhos são baseados nos princípios da segurança da informação quanto à confidencialidade, integridade e disponibilidade.

Capítulo II
DOS OBJETIVOS

Art. 3º. Esta política tem como objetivo estabelecer as diretrizes e padrões para o uso seguro, eficiente e estratégico das informações geradas, produzidas, utilizadas e prestadas pela FUVS e suas Mantidas, garantindo subsídios técnicos para identificar oportunidades, evitar ou mitigar falhas e facilitar a tomada de decisões. Ainda:

I. Descrever as formas como a FUVS e suas Mantidas utiliza, armazena, trata, compartilha e protege os dados pessoais e sensíveis eventualmente coletados por ela e suas Mantidas, garantindo confidencialidade, integridade e disponibilidade das informações;
II. Definir diretrizes e procedimentos padronizados para o gerenciamento do consentimento de *cookies* nos dispositivos utilizados pela FUVS e suas Mantidas, assegurando a proteção e a segurança dos dados;
III. Definir os requisitos mínimos necessários para manter um ambiente de trabalho organizado e seguro, garantindo a proteção de dados e informações relacionadas a funcionários, clientes, parceiros, prestadores de serviços e propriedade intelectual, evitando o acesso não autorizado, assegurando a privacidade, a confidencialidade, a integridade e a segurança dos dados sob gestão da instituição.

Capítulo III
DA ABRANGÊNCIA

Art. 4º. Esta política se aplica aos administradores, gestores, diretores, conselheiros, funcionários e demais *stakeholders* da FUVS e suas Mantidas no tratamento de dados pessoais e sensíveis de funcionários, pacientes, alunos, familiares, visitantes, fornecedores, prestadores de serviços, bem como aos usuários dos *websites* e aplicativos das instituições.

Art. 5º. Cada uma das unidades da FUVS é controladora dos dados pessoais a que tiver acesso no âmbito desta política.

Capítulo IV
DAS DIRETRIZES GERAIS
Seção I
DA GESTÃO DAS INFORMAÇÕES DA ORGANIZAÇÃO

Art. 6º. A FUVS e suas Mantidas orientam que os comportamentos internos e externos ao ambiente institucional devem ser pautados na postura ética profissional, visando promover a proteção das informações corporativas através de atitudes responsáveis e cuidadosas adotadas por todos envolvidos, tanto dentro quanto fora da instituição.

Art. 7º. A FUVS e suas Mantidas consideram, para tratamento desta política, todas as informações coletadas em seus diversos canais, sejam elas por meio físico ou eletrônico, descrevendo as formas como são utilizadas, armazenadas, tratadas, compartilhadas e protegidas, visando:

I. Garantir segurança e integridade dos dados;
II. Garantir confidencialidade e disponibilidade das informações, criando regras de controle de acesso;
III. Integrar as diversas ferramentas/sistemas disponíveis, visando qualificar os dados e agilizar processos;
IV. Implementar ferramentas/sistemas de inteligência – *business intelligence* – para auxiliar os gestores na formatação de estratégias e na execução de planos de ação;
V. Formar uma cultura organizacional robusta, com foco em resultados e que priorize a gestão das informações.

Seção II
DOS TIPOS DE INFORMAÇÕES GERADAS, COLETADAS E UTILIZADAS PARA ALIMENTAR OS PROCESSOS INTERNOS E EXTERNOS DE TODA A ORGANIZAÇÃO E DOS MÉTODOS DE OBTENÇÃO

Art. 8º. Para prestação dos serviços, a FUVS e suas Mantidas podem coletar as seguintes informações pelos meios físicos e/ou eletrônicos:

I. **Informações de pacientes:** Dados pessoais e sensíveis que são necessários para a prestação dos serviços de atendimento clínico e hospitalar, bem como para fins administrativos relacionados aos serviços prestados. Essas informações incluem dados cadastrais como nome, RG, CPF, endereço, data de nascimento, estado civil, religião, gênero, informações para contato, informações financeiras, informações sobre plano de saúde, histórico médico, histórico familiar de doenças, estilo de vida, informações sobre tratamentos realizados, resultados de exames laboratoriais e de imagem e eventuais diagnósticos. Essas informações podem ser coletadas diretamente de pacientes como também prestadas por terceiros, a exemplo de familiares, acompanhantes ou de outros prestadores de serviços.

II. **Informações de terceiros:** Dados de familiares, visitantes, voluntários, profissionais de saúde, responsáveis financeiros de aluno e/ou representante legal, pesquisadores ou prestadores de serviços relacionados à FUVS e suas Mantidas.

III. **Informações de alunos:** Dados necessários para a prestação dos serviços educacionais, bem como para fins administrativos relacionados aos serviços prestados. Essas informações incluem dados cadastrais como nome, RG, CPF, endereço, data de nascimento, gênero, informações para contato, informações financeiras, histórico escolar, captura de imagens para identificação e acesso, histórico médico, histórico familiar de doenças, estilo de vida, informações sobre tratamentos realizados e podem ser coletadas diretamente do aluno e/ou de seu representante legal.

IV. **Informações de funcionários:** Dados pessoais que são necessários para o processo seletivo de candidatos a vagas disponíveis na **FUVS** e suas Mantidas e/ou para a admissão. São elas: nome, CPF, RG, PIS, CNH, CTPS, título de eleitor, certificado militar, escolaridade, diplomas e certificados, registro profissional, foto 3x4, gênero, cor da cútis, data de nascimento, naturalidade, nacionalidade, número de telefone, informações financeiras para efeito de cálculo de impostos, endereço, estado civil, número de conta bancária, cartão de vacinação, cartão do SUS, informações de saúde, exames médicos, de imagens e laboratoriais, captura de imagens para identificação, registro de ponto e acesso. Também são coletadas informações de dependentes e cônjuge/companheiro, tais como: CPF, certidão de nascimento, certidão de casamento, comprovante escolar.

V. **Informações de navegação, registros de acesso e demais informações automatizadas:** Serão armazenadas algumas informações automaticamente toda vez que há interação com os sites, aplicativos, mídias sociais e anúncios da **FUVS** e/ou suas Mantidas. Internet Protocol (IP), tipo de navegador, páginas visualizadas, termos de busca, informações específicas de dispositivos móveis que acessam o site e/ou aplicativo e localização geográfica são alguns exemplos dessa coleta. As datas e horas das interações do usuário com o *site*, aplicativo e *sites* de terceiros também são armazenadas.

VI. **Informações coletadas por meio de aplicativos:** As informações pessoais coletadas dependem do contexto de suas interações com a FUVS e suas Mantidas e com os aplicativos, nas escolhas que o cliente, aluno ou paciente ou usuários fazem e os produtos e recursos que usam. Por esta razão:

   a. Poderão ser coletadas informações pessoais fornecidas como nome, endereço de *e-mail*, endereço postal, número de telefone, informações de contato, senhas e dados de segurança e informações gerais, incluindo pagamentos;
   b. Poderão ser solicitados acessos ou permissões a certos recursos dos dispositivos móveis pessoais, incluindo o armazenamento de tais dispositivos móveis e outros recursos, sendo facultado a alteração dos acessos ou permissões nas configurações desses dispositivos;
   c. Poderão ser coletadas automaticamente informações dos dispositivos como número do ID, modelo, fabricante, sistema operacional, informações sobre a versão e endereço IP;
   d. Poderão ser solicitados o envio de notificações *push* sobre contas pessoais ou aplicativo móvel, sendo facultado o cancelamento do recebimento desses tipos de comunicação nas configurações dos dispositivos.

Seção III
DA ANÁLISE E TRATATIVA DAS INFORMAÇÕES

Art. 9º. O tratamento de dados pessoais e sensíveis pela FUVS e/ou suas Mantidas tem como finalidade primária o estabelecimento de vínculo contratual, ou a gestão, administração, prestação, ampliação e aprimoramento dos serviços prestados, mas também poderão ser utilizados para:

I. Comunicar com clientes e usuários sobre serviços, ofertas, programas, eventos e promoções da FUVS e suas Mantidas, sendo facultado o cancelamento em caso de desinteresse em receber comunicações de *marketing*;

II. Atender aos interesses legítimos da FUVS e suas Mantidas, sempre no limite do que é esperado pelo titular dos dados, e nunca em prejuízo dos seus interesses, direitos e liberdades fundamentais;

III. Gerenciar as comunicações, determinar a eficácia e otimizar nossa publicidade, analisar os serviços, *sites*, aplicativos móveis e quaisquer outros recursos digitais, de modo a facilitar sua funcionalidade;
IV. Realizar atividades de análise pelos departamentos da FUVS e suas Mantidas;
V. Anonimizar os dados pessoais coletados, elaborar e fornecer relatórios de dados agregados com informações anonimizadas (incluindo compilações, análises, regras e modelos analíticos e preditivos e outros relatórios agregados);
VI. Cumprir obrigações legais ou regulatórias;
VII. Exercer direitos da FUVS e/ou suas Mantidas em processos judiciais, administrativos ou arbitrais;
VIII. Para outras finalidades, às quais fornecemos aviso específico no momento da coleta, ou, de outro modo, conforme autorizado ou exigido por lei.

Art. 10. A FUVS e/ou suas Mantidas podem centralizar os dados pessoais coletados, os quais podem ser utilizados nos demais serviços relacionados a todas as Mantidas da FUVS, respeitadas as finalidades ora dispostas e o consentimento do Titular, sempre que exigido por lei.

Art. 11. A FUVS e/ou suas Mantidas podem compartilhar as informações coletadas por meio das páginas de *Internet* ou mediante contato com os Titulares, nas seguintes hipóteses:

I. Com prestadores de serviços e empresas terceirizadas para nos ajudar a operar, executar, aprimorar, entender, personalizar, dar suporte e anunciar nossos serviços. Quando compartilhamos dados com prestadores de serviços terceirizados, exigimos que eles utilizem seus dados de acordo com nossas instruções e termos ou mediante seu consentimento expresso, quando aplicável;
II. Com autoridades, entidades governamentais ou terceiros, para a defesa dos interesses da **FUVS** e/ou suas Mantidas, em qualquer tipo de conflito, incluindo ações judiciais, reclamações perante órgãos públicos, agências reguladoras e processos administrativos;
III. No caso de transações e alterações estatutárias envolvendo a **FUVS** e/ou suas Mantidas em que a transferência das informações sejam necessárias para a continuidade da prestação dos serviços;
IV. Mediante ordem judicial, ou pelo requerimento de autoridades públicas administrativas que detenham competência legal para a sua requisição;
V. Com a sua autorização, em outros casos não previstos acima, havendo o objetivo de compartilhamento dos dados pessoais e informações, enviamos a você uma notificação com informações a respeito de tal compartilhamento para solicitar o seu consentimento, para finalidade determinada.

Art. 12. A **FUVS** e/ou suas Mantidas podem transferir alguns de seus dados pessoais a prestadores de serviços localizados no exterior, incluindo prestadores de serviços em nuvem.

Parágrafo único: Quando seus dados pessoais são transferidos para fora do Brasil, a FUVS e/ou suas Mantidas adotam medidas apropriadas para garantir a proteção adequada de seus dados pessoais, em conformidade com os requisitos da legislação aplicável de proteção de dados, incluindo cláusulas de proteção e segurança nos contratos celebrados para transferência de dados com terceiros de seus dados pessoais.

Art. 13. Em cumprimento e respeito à legislação aplicável ao tratamento de dados pessoais, a FUVS e/ou suas Mantidas garantem ao Titular os seguintes direitos:

I. **Confirmação da existência de tratamento de dados pessoais:** Mediante requisição do Titular, a FUVS e/ou suas Mantidas concedem a confirmação da existência de tratamento de dados pessoais, nos termos da legislação aplicável;

II. **Acesso aos dados:** O Titular pode requisitar acesso aos seus dados pessoais coletados e que estejam armazenados pela FUVS e/ou suas Mantidas;

III. **Correção de dados incompletos, inexatos ou desatualizados:** O Titular pode, a qualquer momento, solicitar alteração e edição dos seus dados pessoais, por meio das centrais de atendimento da FUVS e/ou suas Mantidas;

IV. **Portabilidade de seus dados pessoais:** Mediante requisição expressa do Titular, a FUVS e/ou suas Mantidas realizam a portabilidade dos dados pessoais a outro fornecedor de serviço, nos termos da legislação aplicável;

V. **Eliminação dos dados pessoais:** O Titular pode solicitar a eliminação de dados pessoais que tenham sido coletados pela FUVS e/ou suas Mantidas a partir do consentimento do Titular, a qualquer momento, mediante manifestação gratuita e facilitada. A eliminação dos dados pessoais somente pode ser completa para dados pessoais que não sejam necessários para a FUVS e/ou suas Mantidas cumprirem com obrigações legais, contratuais, para proteção de seu legítimo interesse e nas demais hipóteses admitidas legalmente;

VI. **Informações sobre uso compartilhado de dados:** As informações sobre o compartilhamento de dados pessoais se encontram nesta Política de Privacidade e Proteção de Dados. A FUVS se coloca à disposição do Titular para a hipótese de esclarecimentos complementares;

VII. **Revogação do consentimento**: O Titular pode revogar o consentimento que tenha dado à FUVS e/ou suas Mantidas para tratamento dos seus dados pessoais para certas finalidades, a qualquer momento, mediante manifestação gratuita e facilitada. Importante informar que os tratamentos realizados anteriormente à revogação do consentimento são ratificados e que o pedido de revogação não implica na eliminação dos dados pessoais

anteriormente tratados e que sejam mantidos pela FUVS com base em outros fundamentos legais.

Parágrafo único: Os direitos acima podem ser exercidos diretamente pelo Titular, também por meio de contato com o(a) Encarregado(a) de Proteção de Dados, no endereço de e-mail [lgpd@fuvs.br].

Seção IV
DO USO DE *COOKIES*

Art. 14. A FUVS e suas Mantidas utilizam *cookies* para facilitar a navegação nos ambientes *website* e aplicativos, adaptando-os aos seus interesses e necessidades e acelerando suas atividades e experiências futuras nos portais. Também são utilizados para compilar informações sobre a utilização das páginas e serviços, visando a melhoria contínua de estrutura e conteúdo.

Art. 15. A FUVS e suas Mantidas disponibilizam alternativas para que os usuários desabilitem a coleta automática de informações por meio de algumas tecnologias, como *cookies* e *caches* por meio das configurações em seus navegadores de *Internet*, No entanto, os usuários são informados e devem estar cientes de que, desabilitando a coleta automática, alguns recursos oferecidos pelo *site*, que dependem do tratamento dos referidos dados, podem não funcionar corretamente.

Art. 16. Dos tipos de *cookies* existentes:

I. **Necessários:** essenciais para que as páginas da FUVS e/ou suas Mantidas carreguem corretamente e permitam que o usuário utilize os *sites* fazendo uso de todas as funcionalidades;

II. **De Desempenho:** ajudam a entender como os visitantes interagem com as páginas da FUVS e/ou suas Mantidas, fornecendo informações sobre as áreas visitadas, o tempo de visita ao site e quaisquer problemas encontrados, como mensagens de erro;

III. **Funcionais:** permitem que as páginas da FUVS e/ou suas Mantidas se lembrem das escolhas de seus usuários, proporcionando experiências personalizadas, permitindo que os titulares assistam a vídeos e utilizem ferramentas sociais de interação com campos para comentários, fóruns, dentre outros;

IV. **De *Marketing*:** são utilizados para fornecer conteúdos relevantes e do interesse dos usuários. Podem ser utilizados para apresentar publicidades direcionadas ou limitar o número de vezes que esta é veiculada no *site*; podem também ser utilizados para permitir a medição da eficácia de uma campanha publicitária, servir para indicar as páginas e sites visitados pelo Titular. A FUVS e/ou suas Mantidas podem compartilhar estas informações com terceiros, tais como agências publicitárias contratadas.

Art. 17. A responsabilidade para que o uso de *cookies* esteja em conformidade com a Lei Geral de Proteção de Dados – LGPD é do Gerente do Departamento de Tecnologia, com apoio técnico de sua equipe, cabendo-lhe ainda, gerenciar o consentimento dos usuários, oferecendo opções claras para aceitar, rejeitar ou ajustar as configurações de suas máquinas.

Seção V
DA MESA E TELA LIMPA

Art. 18. A FUVS e suas Mantidas incentivam os funcionários a manterem as áreas de trabalho e comuns limpas e bem conservadas, reforçando a responsabilidade e o cuidado com o ambiente.

Art. 19. Cada item na área de trabalho deve estar devidamente identificado e organizado, assegurando que os funcionários da FUVS e suas Mantidas tenham um espaço funcional que favoreça o desempenho e a produtividade.

Art. 20. Os funcionários, clientes, terceirizados, prestadores de serviços e outros profissionais presentes nos ambientes físicos e virtuais da FUVS, tem papel essencial na proteção de dados confidenciais, garantindo que práticas adequadas sejam seguidas diariamente, devendo observar as seguintes diretrizes que, reforçam o compromisso com a segurança da informação e a organização no ambiente de trabalho:

I. **Manutenção de Equipamentos:** Dispositivos portáteis e de armazenamento em massa devem ser protegidos e armazenados de maneira segura.
II. **Armazenamento Adequado:** Certifique-se de que sua área de trabalho disponha de locais adequados para o armazenamento de documentos e materiais sensíveis, como gavetas trancadas, armários com fechaduras, cofres ou salas de arquivo.
III. **Evite Deixar Documentos Visíveis:** Não deixe documentos em papel, mídias removíveis (como *pendrives* e HDs externos) ou outros itens sensíveis sobre sua mesa. Isso ajuda a prevenir o acesso não autorizado a informações importantes.
IV. **Evite Exposição de Anotações:** Não deixe anotações, recados e lembretes importantes visíveis, especialmente aqueles colados em seu monitor ou em divisórias, como *post-its*. Isso pode comprometer a segurança das informações.
V. **Uso de Crachá:** Leve seu crachá de identificação sempre com você, garantindo que o acesso a áreas restritas seja controlado.
VI. **Senhas Seguras:** Nunca anote senhas em papéis ou outros locais visíveis. Prefira memorizá-las ou armazená-las em locais seguros, como gerenciadores de senhas virtuais.
VII. **Cuidados Após Reuniões:** Ao sair de uma sala de reunião, verifique se todos os papéis foram retirados, se o quadro branco foi apagado e se as folhas do *flipchart* foram descartadas de maneira apropriada.

VIII. **Mesa Limpa:** Evite fazer refeições ou lanches sobre a mesa de trabalho, e nunca apoie copos com bebidas (inclusive água) sobre ela. Isso ajuda a manter um ambiente limpo e organizado.

IX. **Organização no Final do Expediente:** Ao final do expediente, limpe e organize sua área de trabalho para garantir que nenhum documento ou material importante seja deixado para trás.

X. **Armazenamento Seguro:** Documentos que contêm informações estratégicas, internas ou de alunos, pacientes ou terceiros devem ser guardados em gavetas ou armários trancados quando não estiverem em uso, especialmente ao final do expediente. Isso ajuda a prevenir acessos não autorizados.

XI. **Organização Pessoal:** Mantenha agendas, cadernos e outros itens pessoais em gavetas fechadas. Isso assegura que informações privadas e confidenciais não fiquem expostas.

XII. **Proteção Contra Incêndios:** Materiais altamente importantes ou confidenciais devem ser armazenados em locais seguros e à prova de fogo, como cofres, garantindo que possam ser facilmente recuperados em caso de incêndio ou evacuação.

XIII. **Descarte Seguro de Documentos:** Documentos impressos que contêm informações sensíveis devem ser destruídos completamente, de preferência com fragmentadoras, antes de serem descartados, evitando que dados sejam acessados indevidamente.

XIV. **Evitar Exposição de Papéis:** Evite deixar papéis sobre a mesa que possam ser visíveis de janelas ou corredores. Isso pode comprometer a segurança das informações sensíveis.

XV. **Proteção de Telas:** Se você manuseia informações sensíveis, posicione seu monitor ou *notebook* de forma que pessoas não possam olhar sua tela. Utilize também películas ou filtros de privacidade para proteger as informações exibidas.

XVI. **Cautela ao Usar Impressoras e Copiadoras**: Tenha cuidado ao usar impressoras e copiadoras, garantindo que documentos sensíveis não sejam deixados na área de impressão e que sejam recolhidos rapidamente após a impressão.

XVII. **Organização da Área de Trabalho:** Mantenha a área de trabalho do seu computador limpa e organizada, com arquivos guardados em pastas devidamente identificadas. Isso facilita o acesso e contribui para a segurança dos dados.

XVIII. ***Backup* Seguro:** Realize *backups* constantes dos arquivos importantes, armazenando-os de forma segura. Prefira armazenar os dados na nuvem ou em servidores de arquivos (*file server*), em vez de mantê-los localmente no computador, para reduzir o risco de perda de dados.

XIX. **Criptografia de Disco:** Habilite o recurso de criptografia de disco, como o *Microsoft BitLocker*, em seu dispositivo. Isso protege os dados contra acessos não autorizados, mesmo que o dispositivo seja perdido ou roubado.

XX. **Bloqueio Automático do Computador:** Configure seu computador para bloquear

automaticamente e acionar o protetor de tela após 2 ou 3 minutos de inatividade. O desbloqueio do dispositivo deve ser feito apenas por meio de senha.

XXI. **Bloqueio Manual:** Mesmo com a configuração automática, é recomendável bloquear manualmente o computador sempre que você se afastar da mesa. Isso adiciona uma camada extra de segurança.

XXII. **Desligamento do Computador**: Ao final do dia, desligue o computador, especialmente se ele estiver em rede. Além disso, verifique se não há mídias removíveis conectadas ao dispositivo, como *pendrives* ou HDs externos, para evitar a exposição de dados confidenciais.

Seção VI
DA GESTÃO DA SEGURANÇA DAS INFORMAÇÕES QUANTO AO SEU ARMAZENAMENTO SEGURO, REALIZAÇÃO DE *BACKUP* E RECUPERAÇÃO DE DADOS

Art. 21. Em todas as interações tecnológicas, a segurança da informação deve ser priorizada, valendo-se de senhas fortes, não compartilhando credenciais e seguindo medidas de proteção recomendadas.

Art. 22. Todos os funcionários deverão:

I. Manterem a confidencialidade e a integridade dos dados em todas as operações, não divulgando informações sensíveis a pessoas não autorizadas e utilizando métodos seguros de transferência de dados;

II. Manterem-se atualizados sobre as melhores práticas de segurança da informação, acompanhando as últimas tendências e técnicas de proteção para garantir a eficácia das medidas de segurança;

III. Colaborarem ativamente com a equipe de TI para garantir o uso eficiente dos recursos, reportando problemas, vulnerabilidades e/ou necessidades de suporte de forma oportuna.

Art. 23. A equipe de TI assegurará que a infraestrutura e as soluções de TI sejam confiáveis e resilientes e estejam em conformidade com as regulamentações e leis aplicáveis relacionadas à segurança da informação, privacidade de dados e proteção de informações confidenciais.

Art. 24. A equipe de TI desenvolverá e manterá planos de contingência detalhados para garantir a continuidade das operações em caso de falhas ou incidentes.

Parágrafo único. Esses planos incluirão procedimentos claros para restauração de sistemas críticos, priorização de serviços, alocação de recursos e comunicação eficaz com as partes

interessadas internas e externas, competindo à equipe de TI a revisão e aplicação de testes regulares desses planos, garantindo a prontidão para enfrentar situações adversas.

Art. 25. A **FUVS** e/ou suas Mantidas utilizam os meios disponíveis no mercado e legalmente requeridos para preservar a privacidade dos dados pessoais que coleta, adotando diversas diretrizes sobre padrões de segurança, tais como:

I. Criptografia e anonimização de dados;
II. Proteção contra acesso não autorizado a seus sistemas;
III. Controle e registro de todas as pessoas que acessam cada local onde armazena dados pessoais;
IV. Acordos e compromissos de confidencialidade com todos aqueles que acessam dados pessoais;
V. medidas institucionais como Governança, Código de Ética e Conduta e Políticas de Privacidade atualizadas.

Parágrafo único: Considerando, no entanto, que, mesmo adotando as providências necessárias, nenhuma transmissão de dados é totalmente segura, a FUVS e/ou suas Mantidas incentivam que os Titulares adotem medidas pessoais de proteção dentro do seu próprio ambiente.

Art. 26. Os dados pessoais tratados pela FUVS e/ou suas Mantidas são eliminados quando deixam de ser úteis para os fins para os quais foram coletados, ou quando o Titular solicita sua exclusão, exceto nos casos em que a manutenção dos dados for determinada/autorizada por lei ou regulação aplicável ou, ainda, para subsidiar a FUVS e/ou suas Mantidas em possíveis e futuras ações judiciais, reclamações perante órgãos públicos, agências reguladoras ou administrativas em que precisem comprovar o cumprimento de obrigações legais ou contratuais.

Seção VII
Do acesso à Tecnologia de Informação

Art. 27. O acesso à informação é pilar fundamental dentro da FUVS e suas Mantidas e na estrutura da Tecnologia da Informação (TI), sendo necessário o estabelecimento de princípios claros e direcionamentos essenciais para garantir que o acesso aos sistemas e recursos de TI seja gerenciado de maneira segura, eficaz e transparente, protegendo assim informações confidenciais, prevenindo ameaças cibernéticas e mantendo a integridade das operações da organização.

Art. 28. A proteção ao acesso à tecnologia da informação deve contemplar obrigatoriamente:

I. **Acesso Baseado no Princípio do Menor Privilégio:** O acesso aos sistemas e recursos de TI será concedido de acordo com o princípio do menor privilégio. Isso significa que os

usuários terão acesso somente às informações e funcionalidades necessárias para suas atividades específicas. A concessão de privilégios adicionais será autorizada apenas quando estritamente necessário e de acordo com procedimentos estabelecidos.

II. **Autenticação Forte:** A autenticação será implementada de maneira robusta para garantir que apenas usuários autorizados tenham acesso aos sistemas. Isso envolve a utilização de senhas fortes e outros métodos seguros para verificar a identidade dos usuários.

III. **Monitoramento de Acesso:** O acesso aos sistemas e recursos de TI é monitorado continuamente. Atividades de *login*, navegação e interações serão registradas e revisadas regularmente para identificar atividades suspeitas ou não autorizadas. O monitoramento contribui para a detecção precoce de ameaças cibernéticas e a manutenção da segurança.

IV. **Revogação de Acesso:** O acesso dos usuários será revogado imediatamente após a conclusão de suas responsabilidades ou mudanças em seu *status* de emprego. Isso garante que ex-funcionários ou pessoas não autorizadas não mantenham acesso indevido aos sistemas e recursos de TI.

V. **Acesso a Dados Sensíveis:** O acesso a dados sensíveis exigirá revisão e aprovação pela equipe de gerenciamento e pelo departamento de TI. Isso garante que apenas usuários autorizados tenham acesso a informações sensíveis e confidenciais.

VI. **Acesso Remoto:** O acesso remoto a sistemas e recursos de TI seguirá procedimentos rigorosos. Isso inclui o uso de conexões seguras e autenticação robusta para mitigar riscos associados ao acesso fora do ambiente controlado.

VII. A conceção do acesso remoto só poderá ser liberada mediante autorização formal da diretoria executiva.

VIII. **Acessos de Terceiros:** O acesso de fornecedores e parceiros terceirizados seguirá requisitos específicos. Acordos contratuais garantirão a conformidade com as políticas de segurança da empresa e práticas de segurança equivalentes.

IX. **Monitoramento de Acessos Privilegiados:** Usuários com privilégios elevados serão monitorados de maneira especializada para detectar atividades suspeitas. Isso visa mitigar riscos de abuso de acesso por parte de usuários privilegiados.

X. **Auditorias Regulares:** Auditorias periódicas serão conduzidas para revisar os níveis de acesso dos usuários. Essas auditorias garantem que os acessos estejam em conformidade com as políticas estabelecidas, identificando discrepâncias ou riscos potenciais.

Art. 29. Quanto à f**requência das auditorias, essas serão** conduzidas regularmente para monitorar os níveis de acesso, detectar quaisquer atividades suspeitas e garantir a conformidade com as políticas estabelecidas. É definida da seguinte forma:

I. **Auditorias Trimestrais:** A FUVS realizará auditorias de acesso a cada trimestre. Essas auditorias permitirão uma avaliação regular do acesso aos sistemas e recursos de TI, identificando rapidamente possíveis anomalias ou acessos não autorizados.

II. **Auditorias Adicionais:** Em situações especiais, como em resposta a incidentes de segurança ou mudanças significativas na infraestrutura de TI, auditorias de acesso adicionais poderão ser conduzidas para garantir a integridade dos sistemas e a segurança das informações.

Parágrafo único: A auditoria de acesso é realizada pelo Departamento de TI, por funcionário formalmente designado, com cronograma de atuação, *checklist* dos serviços e com procedimentos documentados, que devem incluir:

I. **Avaliação dos registros de acesso:** Revisão dos registros de atividades de *login*, navegação e interações para identificar qualquer atividade suspeita ou não autorizada.

II. **Comparação com políticas de acesso:** Verificação se os acessos estão em conformidade com as políticas estabelecidas, incluindo princípio do menor privilégio e autorizações especiais.

III. **Identificação de anomalias:** Detecção de padrões incomuns ou acessos não usuais que possam indicar atividades suspeitas.

IV. **Revisão de privilégios:** Avaliação dos privilégios de acesso de usuários para garantir que sejam apropriados e necessários para suas funções.

Art. 30. Após a conclusão das auditorias de acesso, quaisquer discrepâncias, atividades suspeitas ou violações de política serão investigadas. A equipe de TI tomará medidas corretivas, incluindo a revogação de acessos não autorizados ou a revisão de privilégios, conforme necessário. As descobertas das auditorias e as ações de acompanhamento serão documentadas e Mantidas para referência futura.

Seção VIII
DOS TREINAMENTOS E DA DISSEMINAÇÃO DA CULTURA DE SEGURANÇA DA INFORMAÇÃO

Art. 31. A FUVS e suas Mantidas implementarão programas de capacitação, treinamentos e disseminação aos seus funcionários sobre os temas abordados nesta política.

§ 1º. Compete ao Departamento de *Compliance*, em parceria com o Departamento de Recursos Humanos, a formatação dos treinamentos e a sua aplicação junto aos funcionários público-alvo.

§ 2º. Os treinamentos serão estruturados de forma a garantir que todos os participantes compreendam os temas abordados, as legislações pertinentes e possam praticar com segurança o aprendizado.

§ 3º. A periodicidade dos treinamentos será definida pelo Departamento de RH, de acordo com o quantitativo de público-alvo e a disponibilidade de datas para os eventos.

§ 4º. Compete ao Gerente do Departamento de RH supervisionar a adequada capacitação dos funcionários acerca das diretrizes contidas nesta norma.

Art. 32. Todos os novos funcionários deverão passar, no momento da integração, por treinamento e conscientização sobre as práticas de segurança cibernética, abordando os tópicos abaixo:

I. A senha criada para o usuário é de sua própria responsabilidade e deve ser mantida em sigilo, não divulgando para outras pessoas e nem facilitando formas de quebra de sua segurança;
II. A *Internet* disponibilizada na FUVS e suas Mantidas é monitorada e tudo o que for acessado pelo usuário fica registrado nos servidores da Instituição, portanto não deverão ser acessados conteúdos incompatíveis com o trabalho;
III. É vedado realizar *downloads* de filmes ou arquivos grandes e que possam comprometer a performance da rede ou prejudicar o uso dos equipamentos, exceto quando devidamente autorizado pela Coordenação do Departamento de TI;
IV. A senha pessoal deverá ser trocada periodicamente elevar a segurança do sigilo;
V. O e-mail funcional e institucional é uma das formas oficiais de comunicação, devendo ser acessado pelo menos uma vez por dia, mantendo a caixa postal sempre atualizada e organizada;
VI. É vedada a divulgação de correntes, piadas ou mensagens não compatíveis com o trabalho realizado na Instituição;
VII. A FUVS e suas Mantidas disponibilizam máquinas e equipamentos para uso durante a jornada de trabalho e esses deverão ser cuidados, devendo sempre que encerrar o expediente, realizar *log-off* na estação e nos *softwares* utilizados.

Seção IX
DA GESTÃO DE CONSEQUÊNCIAS

Art. 33. Funcionários, prestadores de serviços, fornecedores, parceiros ou outros *stakeholders* que observarem desvios às orientações desta política, poderão relatar o fato diretamente no canal de conduta da FUVS, podendo ou não se identificar.

Art. 34. Internamente, o descumprimento das diretrizes desta política enseja a aplicação de medidas de responsabilização dos respectivos agentes, conforme a gravidade do descumprimento, sendo oferecido o devido direito de defesa.

Art. 35. As apurações serão conduzidas com profissionalismo e envolverão o Departamento de *Compliance* para apoiar no processo de apuração. Todos os relatos serão processados e apurados e, se forem constatadas violações, haverá a aplicação de sanções administrativas aos

envolvidos devidamente após a conclusão do devido processo legal e amplo direito de defesa.

Art. 36. É atribuição do superior imediato adotar providências para apurar atos de desvio de conduta cometidas por funcionários de seu departamento/unidade, com o apoio do Departamento de *Compliance* e, se necessário, também com o apoio do Departamento de Recursos Humanos.

Art. 37. O gestor da área deverá ser informado sempre que ocorrer qualquer ato ilícito grave, para que tome conhecimento dos acontecimentos em sua área e possa tomar as medidas cabíveis e/ou acompanhar o devido processo.

Capítulo V
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 38. Compete a todos os funcionários da FUVS e suas Mantidas compreender o papel da segurança da informação em suas atividades diárias, participar dos programas de conscientização e colaborar direta e/ou indiretamente para evitar situações que resultem em riscos institucionais.

§ 1º. Conselheiros, diretores e demais funcionários deverão observar e zelar pelo cumprimento da presente política e, quando assim se fizer necessário, acionar o Departamento de *Compliance* para consulta sobre situações que envolvam conflitos com esta política ou mediante ocorrências de situações nela descritas.

§ 2º. Todos os funcionários deverão atuar de forma ética e responsável quando tomar conhecimento de incidentes, compartilhando informações com os responsáveis pelo seu tratamento em tempo hábil e tomando todas as ações cabíveis para minimizar os potenciais danos que porventura poderão ocorrer.

Art. 39. O Departamento de *Compliance* deverá cumprir as diretrizes estabelecidas nesta política, mantê-la atualizada de forma que quaisquer alterações no direcionamento da FUVS e suas Mantidas sejam incorporadas e ainda esclarecer dúvidas relativas ao seu conteúdo e a sua aplicação.

Art. 40. Fornecedores e prestadores de serviços deverão ser orientados a observar e zelar pelo cumprimento das melhores práticas de segurança da informação, bem como dos requisitos exigidos contratualmente durante o vínculo com a FUVS e suas Mantidas, de forma que atuem com ética e responsabilidade, compartilhando informações com os responsáveis pelo seu tratamento quando tomarem conhecimento de incidentes que possam gerar riscos institucionais.

Capítulo VI
DA DOCUMENTAÇÃO COMPLEMENTAR

Art. 41 – Constituem documentos e normas que deverão ser observados:

I. Lei nº 13.709/2018 – LGPD – Lei Geral de Proteção de Dados Pessoais;
II. ABNT NBR ISO 27001 – Segurança da Informação;
III. Código Conduta e Ética da FUVS;
IV. Lei nº 12.965, de 23/04/2014 – Marco Civil da *Internet.*

Capítulo VII
DAS SIGLAS E CONCEITOS

Art. 42. No intuito de facilitar a compreensão por parte de quaisquer funcionários que tenham acesso às políticas institucionais, destaca-se abaixo, siglas e conceitos de termos utilizados nesta Política:

- **Segurança da informação:** Conjunto de técnicas e estratégias que visam proteger os ativos de informação de uma instituição.
- ***Stakeholders*:** todos os públicos relevantes com interesses à instituição, ou ainda, pessoas ou empresas que assumam algum tipo de relacionamento, direto ou indireto, em face à FUVS e suas Mantidas.
- **Orientação para resultados:** compromisso com a obtenção de resultados que atendam, de forma harmônica e balanceada, as necessidades de todas as partes interessadas na organização.
- **Anonimização:** Utilização de meios técnicos, razoáveis e disponíveis no momento do tratamento de dados pessoais, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. O dado anonimizado não é considerado dado pessoal para os fins da LGPD.
- ***Cookies*:** *Cookies* são, na terminologia da informática, pequenos arquivos de texto depositados por um *site* servidor no computador do usuário para "memorizar" algumas informações relativas àquela navegação.
- **Dado pessoal:** Informação relacionada a pessoa natural identificada ou identificável. Também são considerados dados pessoais aqueles utilizados para formação do perfil comportamental de determinada pessoa natural.
- **Lei Geral de Proteção de Dados Pessoais (LGPD):** Diploma normativo (Lei nº 13.709, de 14 de agosto de 2018) que dispõe sobre o tratamento de dados pessoais e sensíveis em meios digitais ou físicos realizados por pessoa natural ou por pessoa jurídica, de direito público ou privado, tendo como objetivo defender os titulares de dados pessoais e ao mesmo tempo permitir o uso dos dados para finalidades diversas, equilibrando interesses e harmonizando a proteção humana com o desenvolvimento tecnológico e econômico.
- **Titular de Dados Pessoais (TITULAR):** Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

- **Tratamento de Dados Pessoais (TRATAMENTO):** Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle da informação, modificação, comunicação, transferência, difusão ou extração.

Capítulo VIII
DAS DISPOSIÇÕES GERAIS

Art. 43. As situações não previstas na presente política devem ser submetidas à Diretoria Executiva para deliberação em conjunto com o Conselho Diretor.

Art. 44. O descumprimento das normas e orientações contidas nesta política ensejará a aplicação de medidas de responsabilização dos agentes envolvidos, conforme o nível de responsabilidade e gravidade, sendo fonte de referência para as penalidades os Estatutos, Regimentos e demais normas que regulam a FUVS e suas Mantidas.

Art. 45. A FUVS, por intermédio da Diretoria Executiva, estabelecerá prazos para elaboração de planos e ações citadas nesta política, que necessitem de planejamentos específicos, avaliando e aplicando penalidades em casos de descumprimento dos referidos prazos acordados.

Art. 46. Funcionários, fornecedores ou outros *stakeholders* que observarem quaisquer desvios às diretrizes desta política, poderão relatar o fato nos canais abaixo descritos, podendo ou não se identificar:

I. www.fuvs.br
II. Telefone, ligação gratuita: 0800-591-3457

Art. 47. Esta política entra em vigor na data de sua publicação.

Art. 48. A revisão desta política deverá ocorrer a cada 3 (três) anos, ou excepcionalmente quando o Conselho Diretor assim entender.

Pouso Alegre, 30 de junho de 2025

FUNDAÇÃO DE ENSINO SUPERIOR DO VALE DO SAPUCAÍ

Júlio César da Silva Tavares
Presidente do Conselho Diretor

Daniela dos Santos Zica Noronha

Vice-presidente

Ângelo Junqueira Guersoni
Vogal

FUNDAÇÃO DE ENSINO
SUPERIOR DO VALE DO SAPUCAÍ

COMPLEXO HOSPITALAR SAMUEL LIBÂNIO

UNIVÁS
UNIVERSIDADE DO VALE DO SAPUCAÍ

anglo
POUSO ALEGRE

JOÃO PAULO II
COLÉGIO TÉCNICO

LIMA 1972
Lar Irmã Maria Augusta

www.fuvs.br