1. Esta Política Institucional de Gestão de Dados Pessoais do Sicoob estabelece as diretrizes de proteção aos dados pessoais no âmbito das entidades do Sicoob.

2. Aprovada pelo Conselho de Administração do CCS, a política:

   a) é revisada anualmente em decorrência de alterações legais e regulamentares, reformas estatutárias, fatos relevantes ou sugestões encaminhadas pelas entidades do Sicoob, por proposta da área de Segurança da Informação do CCS à Diretoria Executiva do CCS;

   b) é um documento interno, com valor jurídico e aplicabilidade imediata e indistinta, a partir da sua publicação, aos empregados, prestadores de serviços, parceiros e fornecedores no âmbito do Sicoob.

3. Para fins desta Política, os seguintes conceitos são observados:

   a) *entidades do Sicoob*: as cooperativas centrais e singulares e as entidades *do CCS;*

   b) *entidades do CCS*: Bancoob, empresas controladas e fundação patrocinada, Sicoob Confederação, Fundo de Estabilidade e Liquidez do Sicoob e Instituto Sicoob;

   c) *tratamento de dados pessoais:* toda e qualquer operação com dados pessoais, a exemplo de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração entre outras operações possíveis*;*

   d) *dado pessoal:* informação relacionada à pessoa física identificada ou identificável;

   e) *dado pessoal sensível:* dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa física*;*

   f) *operador:* pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

   g) *controlador:* pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais*.*

   h) *encarregado:* identificado pela sigla DPO (*Data Protection Officer*) é a pessoa indicada pelo controlador pelo tratamento de dados pessoais, conforme definido na Lei 13.709/2018 (Lei Geral de Proteção de Dados – LGPD).

4. As diretrizes de gestão de dados pessoais, privacidade, governança de dados e proteção dos dados pessoais estão detalhadas em normativos específicos e a importância da sua adoção deve ser apresentada aos empregados, prestadores de serviços, parceiros e fornecedores das entidades do Sicoob.

5. As responsabilidades e os limites de atuação dos empregados, prestadores de serviços, parceiros e fornecedores na proteção aos dados pessoais são estabelecidos em normativos específicos, reforçando a cultura interna e priorizando as ações necessárias conforme o negócio.

6. As entidades do Sicoob devem formalizar o comprometimento em adequar-se às leis, zelando pela sua aplicação nos negócios, nas parcerias e nas relações com os titulares dos dados pessoais.

7. As entidades do Sicoob devem promover campanhas de conscientização e treinamentos regulares a seus colaboradores sobre identificação, tratamento e proteção de dados pessoais.

8. O Conselho de Administração está comprometido na proteção dos ativos tangíveis e intangíveis das entidades do Sicoob de acordo com as necessidades de negócio e em conformidade legal, garantindo confidencialidade, integridade, disponibilidade, autenticidade e legalidade no tratamento dos dados pessoais.

9. Os princípios de licitude, finalidade, adequação, proporcionalidade e necessidade, minimização, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas, subsidiariedade e limitação de armazenamento devem ser observados pelas entidades do Sicoob no tratamento de dados pessoais.

10. O relatório de impacto à proteção de dados pessoais é confeccionado pelos DPOs das entidades do Sicoob, com finalidade de apresentar a descrição dos processos de tratamento dos dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais dos titulares dos dados, bem como medidas, salvaguardas e mecanismos empregados para mitigar esses riscos.

11. As entidades do Sicoob devem aplicar o processo de avaliação de riscos de segurança da informação para identificar os riscos associados à perda de confidencialidade, integridade e disponibilidade.

12. As entidades do Sicoob devem aplicar o processo de avaliação de riscos de privacidade para identificar os riscos relativos ao tratamento de dados pessoais.

13. As entidades do Sicoob devem assegurar ao longo de todos os processos de avaliação de riscos que a relação entre a segurança da informação e a proteção de dados pessoais seja adequadamente gerenciada.

14. As entidades do Sicoob devem avaliar as consequências potenciais para a organização e os titulares de dados pessoais, caso sejam materializados os riscos identificados.

15. Os procedimentos de resposta às requisições dos titulares dos dados pessoais devem ser submetidos à área de Segurança da Informação, DPO do CCS, que tem como atribuição o apoio na atuação dos DPOs das cooperativas centrais e singulares no que se refere à definição de processos e orientações gerais sobre respostas, principalmente em aspectos relacionados ao cumprimento dos prazos estabelecidos pela Lei e à qualidade e padronização das informações.

16. As entidades do Sicoob devem fornecer meios apropriados e acessíveis de atendimento aos titulares de dados pessoais e disponibilizar informações claras, descrevendo para eles a abrangência na qual as obrigações são atendidas.

17. As diretrizes de segurança, estabelecidas nas Políticas Institucionais de Segurança da Informação e de Segurança Cibernética, deverão ser observadas durante todo o ciclo de vida do dado pessoal.

18. O tratamento dos dados pessoais, baseado no consentimento do titular, deverá ser realizado mediante manifestação de vontade livre do titular de concordância com o tratamento de dados pessoais na forma declarada.

19. As entidades do Sicoob realizarão a gestão do consentimento nos casos em que o tratamento ocorrer nas hipóteses legais de tratamento do consentimento do titular.

19.1 A revogação do consentimento não compromete a licitude do tratamento já efetuado, com base no consentimento previamente dado, e será realizada por procedimento gratuito e facilitado.

19.2 O tratamento de dados pessoais de menores de 18 anos ocorrerá somente se o consentimento for dado por, pelo menos, um dos pais ou responsável legal.

20. As entidades do Sicoob devem assegurar e documentar que o tratamento dos dados pessoas sejam precisos, completos e atualizados, conforme necessidade para os propósitos aos quais ele é tratado, por meio do ciclo de vida do tratamento de dados pessoais.

21. Os dados pessoais devem ser excluídos de forma segura e permanente, depois que o período de retenção expirar ou não terem finalidade, obedecendo os prazos definidos na legislação vigente.

22. Arquivos temporários criados como resultado do tratamento de dados pessoais devem ser descartados seguindo procedimentos e prazos determinados.

23. As entidades do Sicoob devem ter políticas, procedimentos ou mecanismos documentados para o devido descarte de dados pessoais.

24. O tráfego de dados pessoais para outras organizações deve garantir controles apropriados que assegurem o alcance dos dados aos destinos pretendidos.

25. Convém que as entidades do Sicoob assegurem que os dados pessoais, trafegados em redes de transmissão de dados, sejam criptografados.

26. Convém que as entidades do Sicoob assegurem que o uso de dispositivos móveis não conduza a um comprometimento dos dados pessoais.

27. O tratamento de dados pessoais sensíveis é precedido de relatório de impacto à proteção dos dados pessoais.

27.1 O tratamento de dados pessoais sensíveis poderá ocorrer com o consentimento dado pelo titular, realizado de forma específica e destacada, para finalidades específicas.

27.2 O tratamento de dados pessoais sensíveis poderá ocorrer sem o consentimento do titular dos dados pessoais nas hipóteses previstas na LGPD, quando for indispensável o tratamento.

28. Os dados de saúde poderão ser compartilhados, pelas entidades, com outros controladores, considerando o benefício dos interesses dos titulares e se for realizado conforme as exclusividades previstas na LGPD.

29. Projetos e desenvolvimento de sistemas devem incluir diretrizes para as necessidades de tratamento de dados pessoais.

30. As entidades do Sicoob, na figura de controladoras, sempre que fizerem uso de um operador para realizar o tratamento de dados pessoais em seu nome, deverão estabelecer contrato com base na legislação vigente que assegurem o correto tratamento e proteção de dados pessoais.

31. Os colaboradores, prestadores de serviço e DPOs das entidades do Sicoob notificarão, ao DPO do CCS, tempestivamente, sobre qualquer violação ou tentativa de violação de dados pessoais da qual tenham conhecimento.

32. As entidades do Sicoob devem estabelecer acordo de confidencialidade com os colaboradores que tenham acesso aos dados pessoais.

33. As responsabilidades específicas dos envolvidos no tratamento de dados pessoais no Sicoob serão detalhadas no Manual de Gestão de Dados Pessoais.

34. Complementam esta Política e a ela se subordinam todas as normas e procedimentos operacionais que regulam a gestão de dados pessoais no âmbito das entidades do Sicoob.

35. As normas legais prevalecerão sobre esta Política sempre que houver divergência ou conflito.