Portaria Nº 165/2026/IPAM-DRFP

Porto Velho, 18 de março de 2026.

Aprova o manual, que dispõe sobre os procedimentos de controle de acesso físico e lógico aos ativos de informação do Instituto de Previdência e Assistência dos Servidores do Município de Porto Velho – IPAM e dá outras providências.

A DIRETORA PRESIDENTE DO INSTITUTO DE PREVIDÊNCIA E ASSISTÊNCIA DOS SERVIDORES DO MUNICÍPIO DE PORTO VELHO – IPAM, no uso de suas atribuições legais, e considerando o disposto na Política de Segurança da Informação do IPAM e a necessidade de regulamentar o controle de acesso físico e lógico para proteger a confidencialidade, integridade e disponibilidade dos dados e sistemas da instituição,

RESOLVE:

CAPÍTULO I DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Portaria estabelece os procedimentos e requisitos para gerenciar e monitorar o acesso de pessoas e sistemas aos ativos de informação do IPAM, garantindo o princípio do menor privilégio.

Art. 2º As disposições desta Portaria aplicam-se a todos os indivíduos que interagem com os ativos de informação do IPAM, bem como aos próprios ativos, conforme definido na Política de Segurança da Informação.

CAPÍTULO II DO CONTROLE DE ACESSO FÍSICO

Art. 3º O acesso às dependências do IPAM é restrito a servidores, colaboradores, estagiários e visitantes devidamente identificados e autorizados.

§ 1º Todos os indivíduos devem portar sua identificação funcional ou de visitante em local visível durante sua permanência nas instalações.

§ 2º A entrada de visitantes deve ser controlada e registrada, com acompanhamento por servidor responsável.

Art. 4º Áreas que contêm ativos de informação críticos, como salas de computadores e servidores, arquivos físicos com documentos sensíveis e salas de controle, possuem controles de acesso físico mais rigorosos.

§ 1º O acesso a essas áreas é limitado a pessoal autorizado e essencial para a operação, com registro de entrada e saída.

§ 2º O uso de crachás, biometria e chaves é obrigatório para o acesso a áreas restritas.

§ 3º A perda ou extravio de qualquer meio de acesso deve ser comunicada imediatamente à Chefia de Gabinete e à Área de Tecnologia da Informação (CPD).

CAPÍTULO III DO CONTROLE DE ACESSO LÓGICO

Art. 5º O acesso aos recursos digitais do IPAM é concedido com base na necessidade de trabalho e na função de cada usuário.

§ 1º Todos os acessos são individualizados e rastreáveis, exigindo autenticação para garantir a identidade do usuário.

§ 2º A concessão de acesso lógico deve seguir o princípio do menor privilégio, ou seja, cada usuário deve ter apenas o nível de acesso mínimo necessário para desempenhar suas funções.

§ 3º Privilégios adicionais são concedidos apenas mediante solicitação formal e aprovação do gestor da área e da Área de Tecnologia da Informação (CPD), e são revisados periodicamente.

Art. 6º A gestão de senhas e autenticação observará as seguintes diretrizes:

I – As senhas devem atender a requisitos mínimos de complexidade, incluindo comprimento mínimo, uso de caracteres maiúsculos, minúsculos, números e símbolos;

II – Os usuários são obrigados a trocar suas senhas periodicamente, conforme política de segurança estabelecida pela Área de Tecnologia da Informação (CPD);

III – Para sistemas e informações consideradas de alto risco, a autenticação multifator (MFA) pode ser exigida, adicionando uma camada extra de segurança além da senha.

Art. 7º A segregação de funções será implementada para evitar que uma única pessoa tenha controle sobre todas as etapas de um processo crítico, distribuindo responsabilidades e privilégios de acesso entre diferentes indivíduos.

CAPÍTULO IV DA GESTÃO DE IDENTIDADES E CREDENCIAIS

Art. 8º O processo de criação de novas contas de usuário é formalizado, exigindo aprovação do gestor da área e da Área de Tecnologia da Informação (CPD), e baseando-se na necessidade de acesso.

§ 1º Modificações em perfis de acesso são realizadas apenas mediante solicitação justificada e aprovação.

§ 2º A exclusão ou desativação de contas é imediata em casos de desligamento do colaborador ou mudança de função que elimine a necessidade de acesso.

Art. 9º Auditorias e revisões periódicas dos privilégios de acesso serão realizadas pela Área de Tecnologia da Informação (CPD) e pela Controladoria Geral para verificar se os direitos concedidos ainda são apropriados e necessários para as funções atuais dos usuários.

§ 1º Acessos indevidos ou desnecessários serão prontamente removidos.

CAPÍTULO V DOS CONTROLES ESPECÍFICOS DE COMUNICAÇÃO E ACESSO EXTERNO

Seção I Do Canal Corporativo via WhatsApp

Art. 10. É vedado o uso de WhatsApp pessoal para comunicações oficiais do IPAM, incluindo grupos informais entre servidores para tratar de assuntos institucionais.

Art. 11. Qualquer canal via WhatsApp para fins institucionais deve ser previamente aprovado pela Diretoria de Presidência e gerenciado exclusivamente pela Área de Tecnologia da Informação (CPD).

§ 1º Caso seja instituído canal corporativo via WhatsApp, este deve utilizar WhatsApp Business com número institucional.

§ 2º Deverá ser implementada criptografia ponta a ponta e backup seguro das conversas.

§ 3º A Controladoria Geral realizará monitoramento periódico do conteúdo para garantir conformidade com a Lei nº 13.709/2018 (LGPD).

§ 4º Será fornecido treinamento obrigatório aos usuários sobre o uso adequado da ferramenta.

Seção II Dos E-mails Setoriais Não Institucionais

Art. 12. É expressamente proibido o uso de e-mails pessoais ou não institucionais (ex.: gefin@gmail.com, coordenacao@hotmail.com) para comunicações oficiais do IPAM.

§ 1º Toda comunicação oficial deve utilizar exclusivamente endereços corporativos (@ipam.ro.gov.br).

§ 2º O descumprimento do disposto neste artigo sujeitará o servidor às penalidades previstas na Lei Complementar nº 385/2010, além da responsabilização por eventual vazamento de dados previdenciários sensíveis.

CAPÍTULO VI DAS RESPONSABILIDADES

Art. 25. A Área de Tecnologia da Informação (CPD) é responsável por:

I – Implementar e manter os controles técnicos de acesso físico e lógico;

II – Gerenciar as identidades e credenciais dos usuários;

III – Realizar as revisões periódicas de acessos.

Art. 26. A Controladoria Geral é responsável por:

I – Supervisionar a conformidade dos controles de acesso;

II – Realizar auditorias de acessos, especialmente os bancários e de sistemas da Prefeitura;

III – Verificar a efetivação das restrições de acesso em casos de afastamento, mudança de atribuições ou desligamento de servidores.

Art. 27. Os Gestores de cada área são responsáveis por:

I – Aprovar as solicitações de acesso a sistemas e informações para seus colaboradores, garantindo o princípio do menor privilégio;

II – Comunicar imediatamente à Área de Tecnologia da Informação (CPD) e ao Setor de Gestão de Pessoas (GEAD) sobre afastamentos, mudanças de atribuições ou desligamentos de servidores.

Art. 28. O Setor de Gestão de Pessoas (GEAD) é responsável por:

I – Formalizar as alterações de vínculo ou função dos servidores;

II – Coordenar com a Área de Tecnologia da Informação (CPD) a suspensão ou modificação de acessos.

Art. 29. Todos os servidores e colaboradores do IPAM têm o dever de:

I – Cumprir todas as políticas, normas e procedimentos de controle de acesso;

II – Proteger suas credenciais de acesso (senhas, crachás) e não as compartilhar com terceiros;

III – Reportar imediatamente à Área de Tecnologia da Informação (CPD) e à Controladoria Geral quaisquer irregularidades ou suspeitas de acesso indevido.

CAPÍTULO VII DAS SANÇÕES

Art. 30. O descumprimento das diretrizes estabelecidas nesta Portaria, intencional ou por negligência, poderá acarretar sanções disciplinares, administrativas e/ou legais, conforme previsto no item 7.1.2 da Política de Segurança da Informação do IPAM e na Lei Complementar nº 385/2010.

§ 1º As sanções serão aplicadas de acordo com a gravidade da infração, o impacto gerado, a reincidência e as normas internas do IPAM.

§ 2º O descumprimento das diretrizes pode expor o IPAM e o indivíduo responsável a responsabilidades civis e criminais, especialmente em casos de vazamento de dados pessoais, conforme previsto na Lei nº 13.709/2018 (LGPD) e demais legislações pertinentes.

CAPÍTULO VIII DAS DISPOSIÇÕES FINAIS

Art. 31. Esta Portaria será revisada e atualizada anualmente, ou sempre que houver mudanças significativas na legislação, na infraestrutura tecnológica do IPAM, nos processos de negócio ou na identificação de novos riscos relevantes.

Art. 32. Os casos omissos serão resolvidos pela Diretoria de Presidência, mediante consulta à Área de Tecnologia da Informação (CPD), à Procuradoria Geral e à Controladoria Geral.

Art. 33. Todos os servidores, empregados públicos, estagiários, terceirizados e demais usuários que possuam acesso a sistemas, redes ou dados institucionais do IPAM deverão assinar Termo de Ciência e Responsabilidade, declarando conhecimento integral das disposições desta Portaria e da Política de Segurança da Informação vigente.

§ 1º A assinatura do Termo de Ciência e Responsabilidade constitui condição obrigatória para concessão e manutenção de acesso aos sistemas institucionais.

§ 2º A Área de Tecnologia da Informação (CPD) manterá registro atualizado dos termos assinados, em meio físico ou eletrônico, para fins de controle e responsabilização administrativa.

§ 3º A recusa injustificada na assinatura do termo implicará na suspensão ou não concessão de acesso aos sistemas institucionais, sem prejuízo de outras medidas administrativas cabíveis.

§ 4º A obrigatoriedade aplica-se tanto aos usuários atualmente ativos quanto àqueles que vierem a ingressar no IPAM após a publicação desta Portaria.

Art. 34. Nenhuma medida que implique cessação, suspensão, bloqueio ou redução de proventos, benefícios ou vantagens será adotada sem a prévia instauração de procedimento administrativo, assegurados o contraditório e a ampla defesa.

§ 1º O interessado será formalmente notificado para apresentar defesa no prazo mínimo de 10 (dez) dias úteis, podendo juntar documentos e requerer diligências.

§ 2º A decisão administrativa deverá ser motivada, com análise expressa dos argumentos apresentados.

§ 3º Da decisão caberá recurso, no prazo de 10 (dez) dias úteis quando se tratar de medida que implique cessação de pagamento.

§ 4º Em situações de indício de fraude ou irregularidade grave que exijam medida cautelar imediata, poderá ser adotada suspensão provisória devidamente fundamentada, devendo o interessado ser notificado para manifestação no prazo máximo de 5 (cinco) dias úteis, sob pena de nulidade da medida.

Art. 35. Esta Portaria entra em vigor na data de sua publicação.

CLAUDINEIA ARAÚJO DE OLIVEIRA BORTOLETE
Diretora-Presidente

Documento assinado eletronicamente por **Claudineia Araújo de Oliveira Bortolete**, **Presidente**, em 18/03/2026, às 12:23, conforme art. 17, § 1º, do Decreto nº 21.393, de 07 de outubro de 2025.

A autenticidade do documento pode ser conferida no site https://www.portovelho.ro.gov.br/sei informando o código verificador **0674508** e o código CRC **8D446020**.

011.000253/2026-00	0674508v4