VI – programas de computador;
VII – códigos-fonte;
VIII – logs de acesso e registros de auditoria de sistemas;
IX – painéis, dashboards e ferramentas de visualização;
X – metodologias, fluxos e procedimentos técnicos;
XI – documentos administrativos e estratégicos;
XII – notas técnicas, pareceres, apresentações e materiais correlatos;
XIII – quaisquer outros materiais produzidos no exercício das atribuições institucionais da SUPESP.

CAPÍTULO II
DA TITULARIDADE DOS PRODUTOS TÉCNICOS E PROGRAMAS DE COMPUTADOR

Art. 4º. Os produtos técnicos institucionais produzidos no âmbito da SUPESP, durante a vigência de vínculo funcional, contratual, acadêmico ou institucional, pertencem exclusivamente à Administração Pública Estadual, nos termos da legislação aplicável.

Art. 5º. Nos termos do art. 4º da Lei Federal nº 9.609/1998, pertencem exclusivamente à Administração Pública os direitos relativos aos programas de computador, sistemas, códigos-fonte, aplicações, scripts, automações e soluções tecnológicas desenvolvidos:
I – durante a vigência de vínculo estatutário, contratual ou institucional;
II – no exercício das atribuições funcionais;
III – mediante utilização de recursos, dados, infraestrutura ou informações institucionais;
IV – em decorrência da natureza das atribuições exercidas junto à SUPESP.
Parágrafo único. O disposto neste artigo aplica-se igualmente a bolsistas, estagiários, terceirizados e colaboradores.

Art. 6º. É vedada a utilização indevida, exploração econômica não autorizada, cessão, compartilhamento externo irregular, retenção indevida ou divulgação não autorizada de produtos técnicos institucionais, ressalvadas as hipóteses previstas em lei, os deveres de transparência pública, o atendimento à Lei de Acesso à Informação e os compartilhamentos institucionais formalmente autorizados.

CAPÍTULO III
DAS RESPONSABILIDADES DOS AGENTES PÚBLICOS E COLABORADORES

Art. 7º. São deveres dos agentes abrangidos por esta Portaria:
I – preservar o sigilo das informações institucionais;
II – proteger documentos físicos e digitais sob sua guarda;
III – utilizar sistemas e recursos institucionais exclusivamente para fins funcionais;
IV – zelar pela integridade, autenticidade e disponibilidade das informações;
V – observar as normas de segurança da informação e proteção de dados;
VI – comunicar imediatamente incidentes de segurança, acessos indevidos, extravios ou vazamentos de informação;
VII – manter sob sigilo credenciais, senhas e mecanismos de autenticação;
VIII – devolver documentos, equipamentos, mídias e acessos institucionais quando do desligamento ou sempre que solicitado;
IX – observar os níveis de classificação e restrição de acesso das informações institucionais.

Art. 8º. O acesso a sistemas, bancos de dados, documentos e produtos técnicos institucionais deverá observar o princípio da necessidade de conhecimento e limitar-se às atribuições funcionais do usuário.

CAPÍTULO IV
DAS CONDUTAS VEDADAS

Art. 9º. É vedado aos agentes abrangidos por esta Portaria:
I – divulgar, compartilhar, reproduzir, encaminhar ou permitir acesso não autorizado a documentos, relatórios, pesquisas, bancos de dados ou informações institucionais, ressalvadas as hipóteses legalmente autorizadas de transparência, acesso à informação e compartilhamento institucional;
II – utilizar informações, sistemas, programas, infraestrutura tecnológica ou recursos materiais da SUPESP para fins particulares ou estranhos ao interesse público;
III – subtrair, destruir, inutilizar, ocultar, alterar, desfigurar ou reter documentos, registros ou informações institucionais;
IV – remover documentos físicos ou digitais sem autorização;
V – compartilhar senhas, credenciais, certificados digitais, tokens ou mecanismos de autenticação institucional;
VI – permitir ou facilitar acesso de pessoas não autorizadas a sistemas ou bases de dados institucionais;
VII – utilizar indevidamente acessos restritos;
VIII – armazenar documentos institucionais em dispositivos, contas pessoais, serviços de nuvem ou plataformas não autorizadas;
IX – encaminhar documentos institucionais para e-mails pessoais sem autorização formal;
X – utilizar softwares, aplicações ou ferramentas tecnológicas não autorizadas para tratamento de informações institucionais;
XI – inserir, processar, compartilhar ou submeter dados pessoais, dados sensíveis, informações sigilosas, estratégicas ou protegidas por restrição de acesso em ferramentas de inteligência artificial generativa não autorizadas institucionalmente ou em desacordo com as normas de segurança da informação vigentes;
XII – apresentar como de autoria exclusiva própria produtos técnicos desenvolvidos no exercício das atribuições institucionais;
XIII – retardar propositalmente a entrega de produtos técnicos ou a transferência de conhecimento quando da cessação do vínculo;
XIV – manter consigo, após desligamento funcional ou contratual, cópias físicas ou digitais de documentos, sistemas, relatórios, pesquisas, bancos de dados ou quaisquer produtos institucionais sem autorização formal.
Parágrafo único. O uso institucional de ferramentas de inteligência artificial deverá observar supervisão humana, rastreabilidade, revisão técnica e conformidade com a legislação de proteção de dados pessoais e acesso à informação.

CAPÍTULO V
DA SEGURANÇA DA INFORMAÇÃO

Art. 10. Os documentos e produtos técnicos institucionais deverão observar critérios de confidencialidade, integridade, autenticidade, rastreabilidade, disponibilidade, proteção de dados pessoais e segurança da informação, observados os princípios da finalidade, necessidade, adequação e prevenção.

Art. 11. O compartilhamento externo de informações institucionais dependerá de autorização da autoridade competente, ressalvadas as hipóteses de divulgação obrigatória previstas em lei, e observadas as normas legais aplicáveis ao sigilo, proteção de dados pessoais e acesso à informação, zelando pela finalidade pública e o interesse social do compartilhamento.
Parágrafo único. O compartilhamento de dados pessoais sensíveis poderá ser submetido à análise do Comitê Setorial de Proteção de Dados Pessoais - CSPD da SUPESP, conforme regulamentação interna e avaliação de risco aplicável.

Art. 12. A utilização de equipamentos particulares para armazenamento ou tratamento de informações institucionais dependerá de autorização expressa da área competente.

Art. 13. Os acessos concedidos aos sistemas institucionais são pessoais e intransferíveis, sendo o usuário responsável pela utilização de suas credenciais.

Art. 14. Os acessos aos sistemas institucionais poderão ser monitorados e auditados para fins de segurança da informação, continuidade administrativa, prevenção de incidentes e apuração de irregularidades, observados os princípios da proporcionalidade, necessidade e proteção de dados pessoais.

CAPÍTULO VI
DA RESPONSABILIZAÇÃO

Art. 15. O descumprimento das disposições desta Portaria poderá ensejar responsabilização administrativa, civil e penal, sem prejuízo da obrigação de reparação dos danos eventualmente causados à Administração Pública ou a terceiros.

Art. 16. Sem prejuízo das demais normas aplicáveis, constituem fundamentos de responsabilização:
I – o art. 18 da Lei nº 9.826/1974;
II – o art. 31 da Lei Estadual nº 15.175/2012;
III – o art. 18 do Decreto Estadual nº 31.198/2013;
IV – os arts. 154, 154-A, 314 e 325 do Decreto-Lei nº 2.848/1940;
V – a legislação relativa à proteção de dados pessoais (Lei nº 13.709/2018), propriedade intelectual e segurança da informação.

Art. 17. Verificada a ocorrência de irregularidade, poderá ser instaurado procedimento administrativo para apuração de responsabilidade, sem prejuízo da comunicação aos órgãos competentes.

CAPÍTULO VII
DAS DISPOSIÇÕES FINAIS

Art. 18. Esta Portaria será aplicada em caráter complementar à Política de Segurança da Informação da SUPESP, instituída pela Portaria nº 064/2021-SUPESP, e à Política de Gestão de Riscos, instituída pela Portaria nº 063/2021-SUPESP, sem prejuízo da observância das demais normas legais e regulamentares aplicáveis.