PORTARIA Nº 127, DE 24 DE JULHO DE 2017.

Dispõe sobre a Política de Segurança da Informação e Comunicações do Instituto Evandro Chagas (POSIC/IEC).

O Diretor do Instituto Evandro Chagas, no uso de suas atribuições e da competência que lhe foi delegada pela Portaria do MS/nº 256, de 23 de fevereiro de 2016, e

Considerando o Decreto nº 3.505, de 13 de junho de 2000, que Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

Considerando a IN01/DSIC/GSI/PR, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

Considerando a norma ABNT NBR ISO/IEC 27002:2013, Código de Prática para controles de segurança da informação;

Considerando a Portaria nº 271, de 27 de janeiro de 2017, que institui a Política de Segurança da Informação e Comunicações no Ministério da Saúde;

Considerando a importância que deve ser dada à garantia da integridade, à disponibilidade, à confidencialidade e à autenticidade dos dados e das informações nos mais diversos suportes utilizados pelo Ministério da Saúde; e

Considerando o Acórdão nº 1.233 - TCU/2012, que trata da adoção dos normativos de Segurança da Informação e Comunicações (SIC), não facultativos, mas obrigação da alta administração, e o Acórdão nº 3.051-TCU/2014, que prevê a estratégia geral de Segurança da Informação, resolve:

Art. 1º: Instituir, no âmbito do Instituto Evandro Chagas a Política de Segurança da Informação e Comunicações do IEC (POSIC/IEC), regida pelos objetivos e diretrizes estabelecidos nesta Portaria.

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 2º A Política de Segurança da Informação e Comunicações do IEC, também referida como POSIC/IEC institui diretrizes, responsabilidades e competências para viabilizar a disponibilidade, integridade, confidencialidade e autenticidade das informações e comunicações, bem como a conformidade, padronização e normatização das atividades de gestão de segurança da informação e comunicações no IEC, visando à proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da Instituição.

Parágrafo único - Os usuários, colaboradores e clientes que tenham acesso às informações do IEC sujeitam-se aos objetivos e às diretrizes de segurança da informação da Política de que trata esta Portaria, assim como são responsáveis por garantir a segurança das informações a que tenham acesso.

CAPÍTULO II

DOS OBJETIVOS

Art. 3º Constituem os objetivos da POSIC/IEC:

I. estabelecer diretrizes a serem seguidas pelo IEC quanto à adoção de normas e procedimentos relacionados à segurança da informação e comunicações;

II. fornecer ao órgão normas para a segurança da informação, instituindo responsabilidades e atitudes adequadas para manuseio, tratamento, armazenamento, distribuição, uso e descarte da informação para controle e proteção contra a indisponibilidade e falta de integridade, bem como o acesso não autorizado a dados e informações;

III. definir diretrizes, normas e procedimentos para estabelecer controles e processos que assegurem a preservar a informação quanto à:

   a) integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;

   b) confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

c) disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;
d) autenticidade: garantia de que a informação foi produzida, modificada ou descartada por uma determinada pessoa física.

CAPÍTULO III

ABRANGÊNCIA

Art. 4º Esta Política aplica-se aos recursos de Tecnologia da Informação e Comunicações (TIC), ambientes e processos de trabalho, estabelecendo responsabilidades e obrigações a todos os agentes públicos do IEC que tenham acesso às informações ou aos recursos de TIC deste órgão.

CAPÍTULO IV

CONCEITOS, DEFINIÇÕES E TERMINOLOGIAS

Art. 5º - Para fins desta Portaria entende-se por:

I. rede local: rede de dados disponibilizada pelo IEC;
II. data center: ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, e sistemas de ativos de rede, como switches, roteadores, e outros;
III. usuário: qualquer indivíduo como servidor público, terceirizado, consultor, auditor, estagiário, prestador de serviço ou qualquer outro que obtiver autorização do responsável pela área interessada para acesso aos ativos de informação da Instituição;
IV. colaborador: qualquer indivíduo, contratado CLT ou prestador de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro da Área de Tecnologia da Informação e Comunicação da Instituição;
V. gestor da informação: qualquer indivíduo ou comitê designado, que será responsável pela gestão da informação. Esse gestor deve ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os usuários sob a sua gestão.

CAPÍTULO IV

CAPÍTULO V

REFERÊNCIAS LEGAIS E NORMATIVAS:

Art. 6º As ações de Segurança da Informação e Comunicações do Instituto Evandro Chagas deverão observar os seguintes requisitos legais e normativos:

I. Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;
II. Decreto nº 3.505, de 13 de junho de 2000, que Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;
III. Lei nº 9.983, de 14 de julho de 2000, que altera o Decreto-Lei nº 2.848, de 7 de setembro de 1940 (Código Penal), que dispõe sobre a tipificação de crimes por computador contra a Previdência Social e a Administração Pública;
IV. Portaria nº 589, de 20 de maio de 2015, que Institui a Política Nacional de Informação e Informática em Saúde (PNIIS);
V. Instrução Normativa nº 01, de 13 de junho de 2008, do Conselho de Defesa Nacional e suas respectivas Normas Complementares publicadas no Diário Oficial da União (DOU) pelo Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSIPR), que disciplina a gestão de segurança da informação e comunicações no âmbito da Administração Pública Federal;
VI. Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações;
VII. ABNT NBR ISO/IEC 27002:2013 - Tecnologia da Informação-Técnicas de Segurança – Código de Prática para controles de segurança da informação;
VIII. Portaria nº 271, de 27 de janeiro de 2017, que institui a Política de Segurança da Informação e Comunicações no Ministério da Saúde.

CAPÍTULO VI

PRINCÍPIOS DA POSIC

Art. 7º As ações e procedimentos relativos à Segurança da Informação e Comunicações do IEC deverão ser norteados seguintes princípios:

I. autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade. Este princípio de gerar características de não-repúdio que garantirá que o emissor não poderá negar da autoria da mensagem;
II. celeridade: as ações de segurança da informação deverão ofertar respostas rápidas a incidentes e falhas com maior Celeridade possível;
III. clareza: as regras de segurança dos ativos de segurança da informação e comunicações devem ser precisas, concisas e de fácil entendimento;
IV. confidencialidade: as informações ser preservadas e somente estarão disponíveis ou reveladas à pessoa, sistema, órgão ou entidade autorizada e credenciada;
V. disponibilidade: as informações estarão disponível para acesso no momento desejado a quem dela necessitar e possuir autorização para acessá-la;
VI. equanimidade: as normas e regras de segurança da informação são obedecidas por todos, sem distinção de cargo ou função;
VII. ética: os direitos dos agentes públicos serão preservados sem o comprometimento da segurança da informação e comunicações;
VIII. finalidade: As normas e regras de segurança da informação consideram a finalidade dos ativos e das informações a que se referirem;
IX. integridade: as informações não devem ser modificadas ou destruídas de maneira não autorizada ou acidental;
X. menor privilégio: restringir o acesso às informações, ao estritamente necessário ao exercício das funções;
XI. privacidade: informações que firam o respeito à intimidade, à integridade e à honra dos cidadãos, não podem ser divulgadas;
XII. publicidade: dar transparência no trato das informações, observados os critérios legais. Divulgar a todos os agentes públicos do IEC as diretrizes e as normas de segurança da informação;
XIII. responsabilidade/obediência: os agentes públicos tem o dever de conhecer e respeitar todas as normas de segurança da informação e comunicações do IEC.

CAPÍTULO VII

DIRETRIZES GERAIS

Art. 8º É dever dos usuários e colaboradores do IEC conhecer e cumprir a POSIC/IEC.

Art. 9º É condição para acesso aos ativos de informação do IEC a adesão formal aos termos desta Portaria, mediante assinatura de Termo de Responsabilidade constante no ANEXO I.

Art. 10º Todo usuário e/ou colaborador do IEC é responsável pela segurança dos ativos de informação e comunicações que estejam sob a sua responsabilidade e/ou guarda e por todos os atos executados com suas identificações, tais como: identificação de usuário da rede (Login), crachá, carimbo, endereço de correio eletrônico, cartão RFID (Radio-Frequency IDentification), identificação biométrica ou assinatura digital.

Art. 11º Os recursos de TIC disponibilizados pelo IEC devem ser utilizados estritamente dentro do seu propósito.

Art. 12º Os contratos de prestação de serviços, firmados pelo IEC devem conter cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta POSIC, devendo ainda, exigir da entidade contratada, a assinatura de Termo de Confidencialidade.

CAPÍTULO VIII

DIRETRIZES ESPECÍFICAS

Art. 13 A política aqui descrita abrange tanto o ambiente informatizado quanto os meios convencionais de processamento, comunicação e armazenamento da informação e devem seguir as seguintes diretrizes:

I. Propriedade da Informação:

a) Toda a informação criada, armazenada, transportada ou descartada pelos usuários e/ou colaboradores do IEC, no exercício de suas atividades, é de propriedade do órgão e é protegida segundo as diretrizes descritas na POSIC/IEC e nas regulamentações em vigor;

b) Na cessão de bases de dados nominais, informação custodiada ou de propriedade do IEC a terceiros, o Gestor da Informação deverá ser consultado e providenciará a documentação formal relativa à cessão ou autorização de acesso às informações antes da sua disponibilização; e

c) Nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação será utilizada deverá, se necessário, providenciar junto à concedente a documentação formal relativa à cessão de direitos sobre informações de terceiros antes de seu uso.

II. Tratamento da Informação:

a) Toda informação criada, manuseada, armazenada, transportada, descartada ou custodiada pelo IEC é de sua responsabilidade e deverá ser classificada e protegida adequadamente, quanto aos aspectos de confidencialidade, integridade, autenticidade e disponibilidade, de forma explícita ou implícita conforme o Decreto nº 7.845, de 14 de novembro de 2012;

b) A classificação da informação é atribuição do Gestor da Informação;

c) Toda informação institucional, se eletrônica, deverá ser armazenada nos servidores de arquivo e bases de dados sob gestão e administração da Área de TIC (SOINF) e, se não eletrônica, mantida em local que a salvaguarde adequadamente;

d) Toda informação institucional, sob a forma eletrônica, estará salvaguardada por meio de cópia de segurança sob administração da Área de TIC do IEC e mantida em local que a proteja adequadamente e garanta sua recuperação em caso de perda da informação original;

e) No descarte de informações institucionais devem ser observadas as políticas, as normas, os procedimentos internos, a classificação que a informação possui, bem como a temporalidade prevista na legislação; e

f) A informação classificada conforme a legislação vigente produzida, armazenada e transportada em meios eletrônicos deve utilizar criptografia compatível com o grau de sigilo, em especial as informações de autenticação dos usuários das aplicações.

g) Toda informação deve ser protegida de forma preventiva, com o objetivo de minimizar riscos às atividades e serviços do IEC, observando o nível de proteção de acordo com o seu valor, sensibilidade e criticidade, elaborando-se, para tanto, sistema de classificação da informação;

h) Toda informação produzida ou recebida pelos usuários como resultado da atividade profissional contratada pelo IEC pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes, devendo ser respeitada a legislação sobre Direitos Autorais.

i) Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos usuários para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

III. Tratamento de Incidentes de Rede:

a) Cabe ao Setor de Informática a responsabilidade pela infraestrutura necessária para fins de registro e resposta aos incidentes de segurança da informação no âmbito da rede corporativa do IEC;

b) A Equipe de Tratamento de Incidentes de Rede (ETIR) será instituída no Setor de Informática; e

c) Todo usuário e/ou colaborador é responsável por notificar, imediatamente, incidentes que afetem a segurança da informação por meio de recursos de TIC ou o descumprimento da POSIC/IEC à ETIR, para que as providências necessárias sejam adotadas a fim de sanar as causas.

IV. Gestão de Risco:

a) Fica estabelecido o Processo de Gestão de Riscos de Segurança da Informação e Comunicações (PGRSIC), com vistas a minimizar possíveis impactos associados aos ativos de informação e comunicações; e

b) O PGRSIC baseia-se nas melhores práticas, na Norma ISO 31.000:2009 - Diretrizes para a implementação da gestão de riscos e na Norma Complementar nº 04/IN01/DSIC/GSI/PR.

V. Gestão de Continuidade:

a) Fica estabelecido o Programa de Gestão de Continuidade de Negócio (PGCN) em segurança da informação e comunicações no âmbito do IEC, visando reduzir a possibilidade de interrupção causada por desastres ou falhas nos recursos de TIC que suportam as operações do IEC; e

b) Todo sistema ou serviço crítico do IEC deverá estar suportado pelo PGCN.

VI. Auditoria e Conformidade:

a) O uso dos recursos de TIC disponibilizados pelo IEC é passível de monitoramento e auditoria, conforme o previsto no item 9.1.4 do acórdão do Tribunal de Contas da União nº 461 de 28 de abril de 2004, que dispõe sobre a análise regular de arquivos logs com utilização, sempre que possível, de softwares utilitários específicos para monitoramento do uso dos sistemas, e serão implementados e mantidos, sempre que possível, mecanismos que permitam a rastreabilidade desse uso;

b) Serão mantidos procedimentos, tais como: trilhas de auditoria, rastreamento, acompanhamento, controle e verificação de acessos para todos os sistemas corporativos e rede interna do IEC.

VII. Controles de Acesso:

a) Os usuários e/ou colaboradores que utilizarem os recursos de TIC deverão possuir conta de acesso, única e intransferível, cuja concessão de acesso será regulamentada em norma específica;

b) Exigir dos usuários e/ou colaboradores a assinatura do Termo de Responsabilidade e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligados, sobre todos os ativos de informações do IEC;

c) O gestor da informação será responsável na determinação e gerenciamento da concessão e revogação dos privilégios de acesso às informações, considerando sempre o princípio do menor privilégio; e

d) A identificação do usuário e/ou colaborador é pessoal e intransferível, qualquer que seja o meio e a forma, e deve permitir o reconhecimento de maneira inequívoca.

VIII. Uso de e-mail:

a) O uso do correio eletrônico do IEC tem seu uso exclusivo por usuários e/ou colaboradores, no exercício de suas funções. As regras de acesso e utilização são definidas por norma específica, em conformidade com esta POSIC e demais orientações e diretrizes de governo.

IX. Acesso à Internet:

a) O acesso à Internet no ambiente de trabalho do IEC está condicionado às necessidades dos usuários e/ou colaboradores no exercício de suas atribuições e será regido por norma específica, em conformidade com esta POSIC/IEC e demais orientações governamentais e legislação em vigor.

X. Gestão de Mudança:

a) Qualquer mudança no ambiente operacional de TIC deverá ser homologada e testada, gerando documentação e registro;

b) Todo processo de gestão de mudanças é composto, no mínimo, pelas fases de Descrição, Classificação, Aprovação, Verificação e Planejamento, Implementação e Avaliação, de maneira a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação e continuidade dos serviços.

XI. Gestão de Ativos de Informação

O IEC deverá manter um processo de Inventário e Mapeamento dos Ativos de Informação objetivando a Segurança das Infraestruturas Críticas que garantem suas informações assim como a classificação adequada dos ativos.

O inventário e mapeamento de ativos de informação subsidiará o conhecimento, valoração, proteção e a manutenção aos ativos de informação, devendo ser atualizado periodicamente e estruturado de modo a possibilitar a criação de Base de Dados de Ativos de Informação atualizada.

XII. Dispositivos Móveis

A utilização de dispositivos móveis portáteis pelos usuários e colaboradores deverá ser realizada no interesse do órgão.

Todo qualquer dispositivo móvel usado para acessar a rede coorporativa do IEC estará submetido aos padrões estabelecidos pelo SOINF.

A utilização de dispositivos móveis de propriedade da instituição será permitida desde que submetida aos padrões estabelecidos, e, na qualidade de proprietária dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O usuário/colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados pelo SOINF.

A utilização do uso de rede banda larga de dispositivos móveis de propriedade do órgão, em conexões seguras criptografadas de redes conhecidas será definido em norma complementar.

É responsabilidade do usuário/colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pelo IEC, notificar imediatamente seu chefe e ao responsável do SOINF. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O usuário/colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar ao IEC e/ou a terceiros.

O usuário/colaborador que deseje utilizar equipamentos portáteis particulares deve solicitar e justificar utilização do mesmo em suas funções profissionais institucionais. A solicitação deverá ser analisada pelo comitê de segurança da Informação, caso sua requisição seja aprovada o usuário/colaborador disponibilizará previamente seu equipamento a verificação pela SOINF, após verificação e constatação de que o equipamento é seguro, o usuário/colaborador assinará termo de responsabilidade de uso do dispositivo no ambiente do IEC.

O IEC deverá prover rede segregada da rede coorporativa para acesso à Internet pelos visitantes.

XIII. Redes Sociais

A utilização institucional das redes sociais nos aspectos relacionados à Segurança da Informação e Comunicações deverá ser objeto de Norma Interna que, além da Segurança

da Informação e Comunicação, abordará a estratégia de comunicação social, o processo de gestão de conteúdo e outros aspectos relevantes.

A normatização interna de uso seguro das redes sociais deverá estabelecer diretrizes, critérios, limitações e responsabilidades na gestão do uso seguro das redes sociais por usuários que tenham permissão para administrar perfis institucionais ou que possuam credencial de acesso para qualquer rede social a partir da infraestrutura das redes de computadores do IEC.

Perfis institucionais mantidos nas redes sociais devem ser administrados e gerenciados por servidor, ou estar sob a coordenação e responsabilidade deste.

O IEC nomeará um servidor público, ocupante de cargo efetivo, para a função de Agente Responsável pela gestão do uso seguro de cada perfil institucional nas redes.

CAPITULO IX

COMPETÊNCIAS E RESPONSABILIDADES

Art. 14 Compete à SOINF a Gestão da Segurança da Informação e Comunicações eletrônicas.

Art. 15 Compete ao Diretor a aprovação das diretrizes da POSIC/IEC e suas regulamentações, que visam preservar a disponibilidade, a integridade e a confidencialidade das informações do IEC.

Art. 16 O IEC nomeará um servidor público que atuará como Gestor de Segurança da Informação e Comunicações (GSIC), com as seguintes competências:

I. Promover cultura de segurança da informação e comunicações;
II. Atribuir aos usuários e colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da POSIC do IEC;
III. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
IV. Propor recursos necessários às ações de segurança da informação e comunicações;
V. Coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;
VI. Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

VII. Manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação e comunicações; e

VIII. Propor Normas e procedimentos relativos à segurança da informação e comunicações no âmbito do órgão ou entidade da APF.

Art. 17 O Comitê Gestor de Segurança da Informação e Comunicações (CGSIC) é constituído por 1 (um) representante, titular e um suplente, de cada uma das áreas.

§ 1º O CGSIC terá as seguintes competências:

I. Assessorar na implementação das ações de segurança da informação e comunicações nas instituições;

II. Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;

III. Propor normas e procedimentos relativos à segurança da informação e comunicações no âmbito do IEC; e

IV. Revisar e analisar periodicamente esta política e as diretrizes e normas dela decorrentes visando a sua aderência e concordância aos objetivos institucionais e às legislações vigentes.

CAPITULO X

DIVULGAÇÃO E CAPACITAÇÃO

Art. 18 O IEC deverá promover ações permanentes de conscientização dos usuários e colaboradores visando à disseminação das diretrizes e normas estabelecidas nesta política.

Art. 19 A POSIC/IEC e as normas deverão ser divulgadas no boletim de serviço e disponíveis na Intranet para todos os usuários.

CAPITULO XI

ATUALIZAÇÃO

Art. 20 Esta POSIC e todos os instrumentos normativos gerados a partir dela devem ser revisados sempre que se fizer necessário, não devendo exceder o período máximo de 2 (dois) anos.

CAPITULO XII

PENALIDADES

Art. 21 O não cumprimento ou violação de um ou mais itens constantes nesta POSIC caracteriza infração funcional e resultará na suspensão temporária ou permanente de privilégios de acesso aos recursos de TIC, em penas e sanções legais impostas por meio de medidas administrativas sem prejuízo das demais medidas administrativas, cíveis e penais cabíveis.

CAPÍTULO XIII

DAS DISPOSIÇÕES FINAIS

Art. 22 Os casos omissos serão resolvidos pelo Comitê Gestor de Segurança da Informação e Comunicações (CGSIC).

CAPITULO XIV

VIGÊNCIA

Art. 23 Esta Portaria entra em vigor na data de sua publicação.

Ananindeua, _____ de _____ de 2017

PEDRO FERNANDO DA COSTA VASCONCELOS
Diretor do Instituto Evandro Chagas

ANEXO I

TERMO DE RESPONSABILIDADE

Eu, _____

Setor: _____

Função: _____

CPF: _____ Identidade: _____

Matricula: _____ Telefone: _____

Declaro haver solicitado acesso à rede corporativa, computadores, Internet e/ou utilização de e-mail coorporativo, me comprometendo a:

a) Acessar a Internet/Intranet somente por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações em estrita observância aos procedimentos, normas e disposições contidas na Política de Segurança da Informação e comunicação que rege o acesso à rede, à Internet/Intranet e a utilização de e-mails, especialmente no que tange os capítulos 8 e 9 da Política de Segurança da Informação e Comunicação do IEC;

b) Utilizar a caixa postal (e-mail) colocada a minha disposição somente por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações, em estrita observância aos procedimentos, normas e disposições contidas na instrução normativa que rege o acesso à Internet/Intranet e utilização de e-mails, sem liberar o acesso a outras pessoas não envolvidas nos trabalhos executados, o que constitui descumprimento de normas legais, regulamentares e quebra de sigilo funcional;

c) Não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior;

d) Manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

e) Não me ausentar da estação de trabalho sem bloqueá-la com senha, garantindo assim a impossibilidade de acesso indevido por terceiros;

f) Não revelar minha senha de acesso de login de rede, de e-mail e/ou de sistemas de informação e tomar o máximo de cuidado para que ela permaneça somente de meu conhecimento, alterando-a utilizando números, caracteres especiais, letras maiúsculas e minúsculas assim que perceber que a mesma pode ter sido descoberta;
g) Responder, em todas as instâncias, pelas consequências das ações ou omissões de minha parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de minha senha ou das transações a que tenha acesso.

Declaro, ainda, estar plenamente esclarecido e consciente que:

1) É minha responsabilidade cuidar da integridade, confidencialidade e disponibilidade das informações sob minha guarda ou uso, devendo comunicar por escrito ao SOINF/IEC e à minha chefia imediata quaisquer indícios ou possibilidades de irregularidades, de desvios ou falhas identificadas nos sistemas de informação ou recursos de rede, sendo proibida a exploração de falhas ou vulnerabilidades porventura existentes;

2) Devo respeitar as normas de segurança e restrições de sistema impostas pelos sistemas de segurança implantados na instituição;

3) Devo cumprir e fazer cumprir os dispositivos da Política de Segurança da Informação e Comunicação do IEC, de suas diretrizes, bem como deste Termo de Responsabilidade.

Constitui infração funcional e penal, enviar ou facilitar o envio por terceiros de e-mails falsos, inserir ou facilitar a inserção de dados falsos, alterar ou excluir indevidamente dados corretos dos sistemas ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano; bem como modificar ou alterar o sistema de informações ou programa de informática sem autorização ou sem solicitação de autoridade competente ficando o infrator sujeito a punição com a demissão, conforme responsabilização por crime contra a Administração Pública, tipificado no art. 313-A e 313-B, do Código Penal Brasileiro (Decreto-Lei 2.848, de 1940).

Declaro, nesta data, ter ciência e estar de acordo com os procedimentos acima descritos, comprometendo-me a respeitá-los e cumpri-los plena e integralmente, além de manter sempre verossímeis os dados da instituição e de minha área de competência.

_____, ____ de _____ de 20_
Local e Data

Usuário	Reservado para SEGEP
_____	_____
Assinatura	Assinatura