MINISTÉRIO DA EDUCAÇÃO
EMPRESA BRASILEIRA DE SERVIÇOS HOSPITALARES -EBSERH
HOSPITAL DE DOENÇAS TROPICAIS DA UNIVERSIDADE FEDERAL DO TOCANTINS – HDT/UFT

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

Estabelecer as diretrizes da Política de Segurança da Informação do Hospital de Doenças Tropicais da Universidade Federal do Tocantins – HDT/UFT, com observância dos princípios da integridade, da confidencialidade e da disponibilidade.

2. APLICAÇÃO

As disposições desta Política aplicam-se a todos os usuários de recursos de tecnologia da informação disponibilizados pelo HDT/UFT. Todos esses atores são responsáveis por garantir a segurança das informações a que tenham acesso.

3. ALINHAMENTO

3.1 Lei nº 12.550, de 15 de dezembro de 2011, que autoriza o Poder Executivo a criar a empresa pública denominada Empresa Brasileira de Serviços Hospitalares - EBSERH;

3.2 Decreto nº 7.082, de 27 de janeiro de 2010, que institui o Programa Nacional de Reestruturação dos Hospitais Universitários Federais – REHUF;

3.3 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;

3.4 Lei nº 9.983, de 14 de julho de 2000, que dispõe sobre a responsabilidade administrativa, civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;

3.5 Lei 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências;

3.6 Lei nº 12.527, de 18 de novembro de 2011, que regulamenta o acesso às informações públicas;

3.7 Decreto Nº 8.638, de 15 de janeiro de 2016, que institui a Política de Governança Digital.

3.8 Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

3.9 Decreto nº 5.482, de 30 de junho de 2005, que dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da administração pública federal, por meio da Rede Mundial de Computadores –Internet;

3.10 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;

3.11 Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações da Administração Pública Federal, direta e indireta, e dá outras providências, e respectivas normas complementares;

3.12 Instrução Normativa GSI/PR nº 02, de 5 de fevereiro de 2013, que dispõe sobre o credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal;

3.13 Norma ABNT NBR ISO/IEC 27001:2013, que estabelece os elementos de um Sistema de Gestão de Segurança da Informação e Comunicações;

3.14 Norma ABNT NBR ISO/IEC 27005:2011, que estabelece diretrizes para o processo de gestão de riscos de segurança da informação;

4. CONCEITOS E DEFINIÇÕES

4.1 **Confidencialidade:** garantia de que o acesso à informação seja obtido apenas por pessoas autorizadas;

4.2 **Integridade:** preservação da exatidão e completude da informação e dos métodos de processamento;

4.3 **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário;

4.4 **Ativo:** a informação e todos os recursos e dispositivos que a manipulam;

4.5 **Segurança da Informação:** preservação da confidencialidade, da integridade e da disponibilidade da informação;

4.6 **Recurso de Tecnologia da Informação:** qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação, bem como as instalações físicas que os abrigam;

4.7 **Usuários:** agentes públicos desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, consultores e ainda os estagiários e menores aprendizes em atividade no HDT/UFT;

4.8 **Plano de Continuidade do Negócio:** conjunto de ações de prevenção e procedimentos de recuperação a serem seguidos para proteger os processos críticos de trabalho contra efeitos de falhas de equipamentos, acidentes, ações intencionais ou desastres naturais significativos, assegurando a disponibilidade das informações;

4.9 **Evento de segurança da informação:** ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da Política de Segurança da Informação ou falhas de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação. [ISO/IEC TR 18044:2004]

4.10 **Incidente de segurança da informação:** é identificado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação. [ISO/IEC TR 18044:2004]

4.11 **Acesso:** ato de ingressar, transitar, conhecer ou consultar a informação, bem como a acessibilidade de usar os ativos de informação de um órgão ou entidade;

4.12 **Ameaça:** qualquer evento que explore vulnerabilidade ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

4.13 **Análise de riscos:** qualquer evento que explore vulnerabilidades ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

4.14 **Atividade:** processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;

4.15 **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;

4.16 **POSIC:** Política de Segurança da Informação e Comunicações (documento aprovado pela autoridade responsável do órgão ou entidade da Administração Pública Federal, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações);

4.17 **Avaliação de riscos:** processo de comparar risco estimado com critérios de risco predefinidos para determinar a importância do risco;

4.18 **Tratamento de incidentes:** é o processo que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes

de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

5. CONTEÚDO

5.1 São de propriedade do HDT/UFT as informações geradas ou manipuladas pelos usuários identificados no item 4.7 desta política, no desempenho de suas funções, ainda que fora das dependências físicas do órgão e independentemente da forma de apresentação ou armazenamento com que tenham sido produzidas.

5.1.1 As informações de que trata o item 5.1 devem ser adequadamente protegidas e utilizadas exclusivamente para os fins relacionados às atividades institucionais no HDT/UFT.

5.1.2 Toda informação gerada ou manipulada no HDT/UFT deve ser classificada de acordo com norma proposta pela Comissão de Segurança da Informação e editada por meio de portaria da Superintendência.

5.1.3 O HDT/UFT adotará dispositivos de proteção capazes de assegurar a autenticidade, integridade e disponibilidade da informação, conforme o seu nível de classificação e independentemente do suporte em que seja armazenada ou veiculada.

5.1.4 Compete à chefia imediata do usuário zelar, no âmbito de sua unidade, pela observância das disposições constantes desta Política, bem como pelas normas relativas à segurança da informação que vierem a ser editadas, comunicando à autoridade superior as eventuais irregularidades.

5.1.5 A inobservância das normas previstas nesta Política será devidamente apurada, podendo ensejar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurado aos envolvidos o contraditório e a ampla defesa.

5.1.6 Os contratos e convênios celebrados pelo HDT/UFT, cujo objeto envolva a utilização de recursos de tecnologia da informação, deverão conter cláusula exigindo a observância desta Política, que estará disponível no sítio eletrônico do HDT/UFT na internet.

5.1.7 O Setor de Gestão da Informação e Informática deverá constituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR.

6. COMPETÊNCIAS E RESPONSABILIDADES

6.1 **Compete à Comissão de Segurança da Informação:**

6.1.1 Coordenar, implantar, divulgar e operacionalizar a Política de Segurança da Informação do Hospital de Doenças Tropicais da Universidade Federal do Tocantins, bem como propor e acompanhar planos de ação para aplicação desta política;

6.1.2 Propor a realização de campanhas de conscientização dos usuários quanto à política de segurança da informação;

6.1.3 Dirimir dúvidas e deliberar sobre questões não contempladas pela política de segurança da informação ou pelas normas a ela relacionadas, bem como sugerir as alterações necessárias;

6.1.4 Deliberar sobre as propostas de atos normativos apresentadas pelo Setor de Gestão da Informação e Informática, relativos às seguintes matérias, entre outras:

I) Acesso aos recursos de rede, inclusive internet;
II) Uso adequado de correio eletrônico (e-mail), estações de trabalho e dispositivos móveis fornecidos pelo HDT/UFT;
III) Uso e instalação de softwares;
IV) Monitoramento e auditoria dos recursos de tecnologia da informação;
V) Tratamento e resposta a incidentes em redes computacionais;
VI) Controle de Acesso Lógico;
VII) Inventário de Ativos de Informação;
VIII) Classificação da Informação;
IX) Controles Criptográficos; e
X) Gestão de Riscos de Segurança da Informação.

6.1.5 Deliberar sobre as iniciativas do Setor de Segurança da Informação relacionadas ao incremento da segurança da informação.

6.1.6 Os atos normativos de que trata o item 6.1.4 serão materializados por meio de Portarias da Superintendência, numerados sequencialmente e publicados no órgão oficial de divulgação do HDT/UFT.

6.2 Compete ao Setor de Segurança da Informação:

6.2.1 Elaboração das normas previstas no item 6.1.4 e encaminhamento à Comissão de Segurança da Informação, para fins de deliberação;

6.2.2 Assessoramento à Comissão de Segurança da Informação, sempre que solicitado pelo seu Superintendente, mediante esclarecimentos técnicos, prestação de informações ou encaminhamento de documentos;

6.2.3 Elaboração de programas de treinamento visando à capacitação dos proprietários e usuários da informação;

6.2.4 Monitoramento e auditoria dos recursos de tecnologia da informação do HDT/UFT;

6.2.5 Análise periódica de riscos relacionados a tecnologia da informação e a seus ambientes, processos e pessoas;

6.2.6 Comunicação à Comissão de Segurança da Informação dos incidentes de segurança tecnológica e do nível de segurança alcançado nos ambientes tecnológicos, por meio de relatórios gerenciais provenientes das análises de risco.

6.3 A Equipe de Tratamento e Resposta a Incidentes de Informação em Redes Computacionais é responsável por:

6.3.1 Receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores, armazenar registros para formação de séries históricas como subsídio estatístico, entre outras competências definidas em normativo próprio.

7. Do serviço de Correio Eletrônico Institucional

7.1 Objetivo

Estabelecer regras e padrões para a utilização do serviço de correio eletrônico

7.2 Conceitos

Para os efeitos desta norma são estabelecidos os seguintes conceitos e definições:

7.2.1 Serviço de correio eletrônico institucional – serviço de envio e recebimento de mensagens eletrônicas (também conhecidas por "e-mails") no âmbito do Hospital de Doenças Tropicais HDT/UFT.

7.2.2 Caixa postal – conta de correio eletrônico onde são armazenadas as mensagens recebidas e/ou enviadas.

7.2.2.1 Caixa postal institucional pessoal – conta de correio eletrônico de um único usuário.

7.2.2.2 Caixa postal institucional da unidade – conta de correio eletrônico de uma unidade administrativa, constante da estrutura organizacional do HDT/UFT.

7.2.2.3 Caixa postal de sistema – conta de correio eletrônico de um sistema informatizado que necessite esse recurso para o seu funcionamento.

7.2.3 Lista de distribuição – agrupamento de diversos endereços eletrônicos, que permite a distribuição conjunta de uma mensagem eletrônica a todos os seus integrantes, sem caixa postal específica.

7.2.4 Endereço eletrônico – conjunto de caracteres que individualiza e identifica o remetente e o destinatário da mensagem eletrônica. É formado por um identificador e por um domínio, separados pelo símbolo arroba (@).

7.2.4.1 Identificador – parte inicial do endereço eletrônico, localizada antes do símbolo arroba (@).

7.2.4.2 Domínio – parte final do endereço eletrônico, localizada após o símbolo arroba (@).

7.2.5 Arquivo de registro de mensagens (logs) – compila registros de eventos relevantes, utilizados para restaurar um sistema, diagnosticar problemas, ou realizar auditorias.

7.2.6 Spam – mensagem enviada a um grande número de endereços eletrônicos, que não possua caráter institucional e/ou cujo objeto não seja inerente à atividade funcional do usuário ou da unidade.

7.2.7 Phishing – fraude eletrônica, caracterizada pela tentativa de obtenção de dados e informações pessoais com o uso de meios técnicos e de engenharia social.

7.2.8 Malware – programas indesejados, desenvolvidos com a finalidade de executar ações danosas e atividades maliciosas em um computador ou sistema (ex.: worm, bot, spyware, backdoor, cavalo de tróia e rootkit).

7.2.9 Material criptografado – dados e/ou informações codificadas por meio de técnicas que impossibilitam o seu entendimento/leitura, cuja reversão ocorre somente com a utilização de uma senha previamente conhecida e/ou dispositivo criptográfico (ex.: token, smart card).

7.2.10 Hoax – mensagem eletrônica encaminhada a muitos destinatários e de conteúdo geralmente alarmante e com pouca ou nenhuma veracidade, cujo objetivo é a propagação de boatos e informações distorcidas.

7.3 Caixas postais de correio eletrônico (criação, alteração e exclusão)

7.3.1 As caixas postais são identificadas unicamente por meio de seu endereço eletrônico.

7.3.2 No âmbito deste HDT/UFT, o domínio do endereço eletrônico é "ebserh.gov.br".

7.3.3 As solicitações de criação, alteração e exclusão de caixas postais devem ser encaminhadas ao Setor de Gestão da Informação e Informática.

7.4 Utilização dos recursos do sistema de correio eletrônico

7.4.1 O uso do correio eletrônico institucional restringe-se a mensagem cujo objeto seja, necessariamente, inerente à atividade funcional do usuário ou da unidade, sendo vedado o uso para fins particulares.

7.4.2 O acesso ao correio eletrônico, a partir de estações de trabalho fornecidas pelo HDT/UFT, será feito pelos navegadores de internet, bem como pelo programa Microsoft Outlook.

7.4.3 É vedada a tentativa de acesso a caixas postais às quais o usuário não tenha autorização de acesso.

7.4.4 É de responsabilidade do usuário:

I) utilizar o correio eletrônico institucional de acordo com os preceitos desta Norma;
II) eliminar periodicamente as mensagens eletrônicas contidas nas caixas postais;
III) manter apenas o seu acesso à conta institucional pessoal de correio eletrônico, sendo vedada a disponibilização desse acesso a terceiros;
IV) informar ao Setor de Gestão da Informação e Informática o recebimento de mensagem que contrarie o disposto no item.

7.4.5 É vedado aos usuários o envio de qualquer mensagem eletrônica contendo:

I) informações privilegiadas, confidenciais e/ou de propriedade do HDT/UFT para destinatários não autorizados;
II) materiais obscenos, ilegais ou antiéticos;
III) materiais preconceituosos ou discriminatórios;
IV) materiais caluniosos ou difamatórios;
V) listagem com endereços eletrônicos institucionais;
VI) malwares (item 7.2.8);
VII) material de natureza político-partidária, associativa ou sindical, que promova a eleição de candidatos para cargos eletivos;
VIII) entretenimentos e "correntes";
IX) assuntos ofensivos;
X) músicas, vídeos ou animações que não sejam de interesse específico do trabalho;
XI) Spam, phishing e hoax (itens 7.2.6, 7.2.7 e 7.2.10);
XII) materiais criptografados.
XIII) propaganda com objetivo comercial;
XIV) material protegido por lei de propriedade intelectual;

8. USO DE RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

8.1 Diretrizes gerais

8.1.1 O uso adequado dos recursos de tecnologia da informação visa a garantir a continuidade das atividades desenvolvidas neste HDT/UFT.

8.1.2 Os recursos de tecnologia da informação disponibilizados pelo Hospital de Doenças Tropicais aos usuários serão utilizados em atividades relacionadas às funções institucionais, e abrangem os seguintes elementos:

I) os computadores servidores, os computadores para uso individual ou coletivo, de qualquer porte, os equipamentos de armazenamento e distribuição de dados, as impressoras, as copiadoras e os equipamentos multifuncionais, assim como os respectivos suprimentos, periféricos e acessórios;

II) a rede lógica do HDT/UFT e os respectivos canais e pontos de distribuição;

III) as contas de acesso dos usuários, assim como os certificados digitais;

IV) os sistemas computacionais desenvolvidos com base nos recursos providos pelo HDT/UFT;

V) os sistemas computacionais contratados de terceiros, sob licença ou na forma de software livre ou aberto, incluídas as soluções baseadas em nuvem.

8.1.3 O usuário é responsável por:

I) zelar pelos recursos que lhe sejam destinados para o exercício de suas atribuições, especialmente os de utilização pessoal, tais como computadores, impressoras, dispositivos móveis e demais equipamentos;

II) preservar o sigilo de sua senha ou outro mecanismo de autenticação que venha a ser utilizado para acesso aos recursos tecnológicos disponibilizados;

III) preservar o sigilo das informações a que tiver acesso, sendo vedada sua revelação a usuários ou terceiros não autorizados;

IV) atos praticados e acessos realizados aos recursos de tecnologia por meio de sua credencial de acesso.

8.1.4 Os procedimentos de instalação, configuração e manutenção de equipamentos e softwares serão realizados pelo Setor de Gestão da Informação e Informática ou por terceiros por ele autorizados, sob a supervisão do gestor da unidade, que verificará a adequação do serviço realizado ao atendimento das atividades desenvolvidas pela unidade.

8.1.5 Não será fornecido suporte a equipamentos particulares (computadores, notebooks, smartphones e tablets), seja quanto à instalação e configuração de sistemas ou aplicativos, ainda que disponibilizados pelo HDT/UFT, seja quanto às questões relacionadas à conexão à rede sem-fio.

8.1.6 Os equipamentos servidores e os computadores para uso individual ou coletivo, de qualquer porte, serão dotados de mecanismos de proteção contra malwares.

8.2 Da Rede Lógica

8.2.1 Todos os equipamentos e dispositivos móveis conectados à rede lógica de dados do HDT/UFT terão seus acessos monitorados por questões de segurança e para fins de auditoria.

8.2.2 A cada ponto de acesso à rede de dados do HDT/UFT poderá ser conectado apenas um equipamento, vedada a utilização de dispositivos multiplicadores de acesso, salvo mediante expressa autorização do Setor de Gestão da Informação e Informática.

8.2.3 É proibida a conexão de qualquer dispositivo não fornecido pelo HDT/UFT na rede cabeada do Hospital, sem a prévia anuência do Setor de Gestão da Informação e Informática.

8.2.3.1 A conexão de qualquer equipamento à rede cabeada do HDT/UFT será feita pelo Setor de Gestão da Informação e Informática, ou por terceiros por ele autorizados.

8.2.4 O HDT/UFT disponibilizará acesso à rede sem-fio para usuários internos e externos.

8.2.4.1. A conexão, para os usuários internos, será feita por meio da credencial (nome de usuário e senha) utilizada para o acesso à rede, e, para os usuários externos, será feita mediante cadastramento prévio em sistema específico do HDT/UFT.

8.2.4.2. É permitida a conexão de dispositivos móveis particulares nas redes sem-fio administradas pelo HDT/UFT.

8.2.4.3. O acesso à internet por meio das redes sem-fio observará as regras da Política de Segurança da Informação.

8.2.4.4. Por questões de segurança tecnológica, regras específicas poderão ser implementadas no acesso à internet via rede sem-fio.

8.2.4.5. Poderão ser bloqueados os acessos à rede sem-fio, temporariamente ou por tempo indeterminado, de dispositivos móveis identificados durante o monitoramento como fonte de ações maliciosas, intencionais ou não, ou em que detectadas vulnerabilidades ou problemas de segurança tecnológica.

8.2.5 Cada unidade do HDT/UFT terá disponível área de armazenamento em rede para salvaguardar os arquivos relacionados ao trabalho desenvolvido, com garantia de integridade, disponibilidade, controle de acesso e cópia de segurança.

8.2.5.1. Os dados armazenados nas estações de trabalho dos usuários não estão contemplados pelas garantias mencionadas nesse item, cabendo aos usuários providenciar eventual cópia de segurança e a eliminação periódica dos arquivos armazenados nos discos rígidos locais.

8.2.5.2. É proibido o armazenamento, em qualquer diretório na rede do HDT/UFT ou nas soluções baseadas em nuvem, de arquivos não relacionados ao trabalho, os quais ficarão sujeitos à exclusão, sem prévio aviso, pelo Setor de Gestão da Informação e Informática, tais como:

I) fotos, músicas e filmes de qualquer formato;

II) programas não homologados ou não licenciados;

III) programas de conteúdo prejudicial à segurança do parque computacional deste Hospital.

8.3 Nuvem corporativa

8.3.1. Ao armazenamento de arquivos na nuvem corporativa aplicam-se as regras previstas no item 8.2.5.2.

8.3.2. Os arquivos armazenados na nuvem corporativa poderão ser compartilhados exclusivamente com outros usuários do HDT/UFT.

8.4 Computadores portáteis fornecidos pelo HDT/UFT

8.4.1. O fornecimento de computadores portáteis aos usuários está condicionado às necessidades de trabalho e à assinatura do Termo de Responsabilidade e Recebimento.

8.4.2. Os computadores portáteis possuem instalação padrão desenvolvida pelo HDT/UFT, composta por softwares e aplicativos necessários ao desempenho das funções de trabalho, além de softwares para proteção, monitoramento e auditoria do equipamento.

8.4.3. Os problemas de software serão solucionados pela reinstalação padrão desenvolvida pelo HDT/UFT, que fica desobrigado de reinstalar e configurar programas que o usuário tenha instalado por iniciativa própria e isento da responsabilidade sobre eventual perda de dados de arquivos pessoais.

8.4.4. A instalação, manutenção e suporte de qualquer software/sistema não fornecido pelo HDT/UFT, bem como o backup de dados locais, é de exclusiva responsabilidade do usuário.

8.4.5. Em caso de exoneração, dispensa da função, cedência, remoção, aposentadoria ou término das atividades que ensejaram o fornecimento, o equipamento deve ser devolvido ao HDT/UFT, com todos os acessórios que o acompanharam, no prazo de 5 dias.

8.5 Licenças de software

8.5.1. As licenças de softwares, de qualquer natureza, contratadas ou adquiridas pelo HDT/UFT são de uso institucional, privativo deste Hospital.

8.5.2. O HDT/UFT utilizará, preferencialmente, em suas atividades, Software Livre ou de Código Aberto.

5.5.2.1. Fica definida como padrão a suíte de escritório Libre Office desenvolvida pela Associação Civil sem Fins Lucrativos BrOffice.org Projeto Brasil.

8.5.3. É proibida a instalação de softwares não licenciados ou não homologados pelo Setor de Tecnologia da Informação e Informática nos equipamentos conectados à rede do Hospital.

5.5.3.1. A instalação de softwares não homologados poderá ser autorizada excepcionalmente pelo SGII, desde que demonstrada a necessidade de sua utilização para o desempenho das atribuições funcionais do usuário, observadas as condições de segurança e proteção estabelecidas, bem como a compatibilidade e adequação aos recursos computacionais disponibilizados pelo HDT/UFT.

5.5.3.2. As unidades organizacionais do HDT/UFT poderão encaminhar ao SGII pedido de homologação de softwares, para o uso em suas atividades.

5.5.3.3. Homologado o uso, o software passará a integrar o padrão utilizado na configuração dos novos equipamentos. Quando necessário, o pedido, acompanhado de parecer técnico, será submetido ao Comitê de Segurança da Informação.

8.6 Serviço de mensagem instantânea

8.6.1. O serviço de mensagem instantânea disponibilizado pelo HDT/UFT destina-se às comunicações internas.

9. Do controle do acesso

9.1 Do gerenciamento de acessos

9.1.1. O acesso à rede, serviços e aos sistemas computacionais disponibilizados pelo HDT/UFT serão solicitados ao Setor de Gestão da Informação e Informática, por meio do sistema de atendimento, em que definidos os níveis de acesso adequados às atividades desenvolvidas.

9.1.2. Incumbe à chefia imediata solicitar ao Setor de Gestão da Informação e Informática:

I) os acessos necessários ao desenvolvimento das atividades dos usuários vinculados a sua unidade.

II) a alteração dos níveis de acesso ou a remoção do acesso a sistemas concedidos aos usuários da unidade, sempre que necessária sua adequação às atividades desenvolvidas.

III) a remoção dos acessos concedidos aos usuários, imediatamente após o afastamento ou desligamento da unidade.

9.1.2.1. Não solicitada a alteração ou exclusão no momento oportuno, a chefia poderá ser responsabilizada pelo acesso indevido do usuário a informações da unidade.

9.1.3. O Setor de Gestão da Informação e Informática comunicará à unidade respectiva sobre a efetivação do cadastro, fornecendo as informações necessárias ao acesso, e encaminhará a Política de Segurança da Informação, em formato eletrônico, para a caixa postal institucional pessoal do usuário, para ciência.

9.1.4. As novas senhas solicitadas serão fornecidas por meio de comunicação eletrônica para a caixa postal institucional da unidade ou caixa postal institucional pessoal do usuário, proibido o fornecimento de senhas por qualquer outro meio, inclusive telefone.

9.1.4.1 É responsabilidade do usuário a alteração da senha inicial fornecida pelo Setor de Gestão da Informação e Informática no primeiro acesso realizado.

9.1.5. A Divisão de Gestão de Pessoas comunicará ao Setor de Gestão da Informação é Informática os casos de falecimento e os afastamentos em decorrência de exoneração, redistribuição, aposentadoria, remoção e cedência a outro órgão, retorno à origem, ou término do estágio de estudantes, para remoção dos acessos concedidos aos usuários.

9.1.6 As solicitações de acessos de prestadores de serviço aos recursos tecnológicos do HDT/UFT terão caráter temporário e deverão ser acompanhadas da respectiva justificativa, bem como do prazo previsto para a realização das atividades.

9.1.7 O privilégio de administrador na estação de trabalho é restrito aos técnicos de informática que necessitem de acesso privilegiado para o desempenho das atividades funcionais.

9.2 Da conta de rede e respectiva senha para utilização

9.2.1. Para ter acesso aos recursos de tecnologia da informação disponibilizados pelo HDT/UFT é necessário que o usuário possua uma conta de rede.

9.2.2. A identificação de usuário será composta pela primeira letra do prenome e o último sobrenome do usuário.

9.2.3. Em situações justificadas, poderá ser utilizado outro prenome ou sobrenome para a composição da identificação.

9.2.4. A cada conta de acesso será associada uma senha, de uso pessoal e intransferível.

9.2.5. Na utilização das credenciais de acesso, compete ao usuário observar os procedimentos a seguir indicados, bem como adotar outras medidas de segurança de caráter pessoal, com vista a impedir o uso não autorizado dos recursos de tecnologia da informação a partir de sua conta de acesso:

I) não compartilhar a senha com outras pessoas;

II) não armazenar senhas em local acessível por terceiros;

III) não utilizar senhas de fácil dedução como as que contém nomes próprios e de familiares, datas festivas e sequências numéricas;

IV) ao ausentar-se de sua estação de trabalho, ainda que temporariamente, o usuário deverá encerrar ou bloquear a sessão.

9.2.6. A senha deverá satisfazer os seguintes requisitos de complexidade:

I) não conter nome da conta do usuário (login) ou mais de dois caracteres consecutivos de partes de seu nome completo;

II) ter pelo menos seis caracteres;

III) conter caracteres de, no mínimo, três das quatro categorias a seguir:

a) caracteres maiúsculos (A-Z);

b) caracteres minúsculos (a-z);

c) dígitos de base (0 a 9);

d) caracteres não alfabéticos (como !, $, #, %).

9.2.6.1. Excetuam-se da regra do item 9.2.6 os sistemas atualmente disponibilizados que não permitam o atendimento aos requisitos estabelecidos.

9.2.7. Em caso de suspeita de comprometimento da senha ou de outro recurso de autenticação, o usuário comunicará imediatamente ao SGII, que poderá, como medida preventiva, suspender temporariamente o acesso.

10. Atualização da Norma

10.1. As diretrizes previstas na presente norma serão atualizadas sempre que alterados os procedimentos de uso de recursos de tecnologia da informação e de controle de acesso, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação.

José Pereira Guimarães Neto
Superintendente
HDT-UFT / EBSERH

MINISTÉRIO DA EDUCAÇÃO
EMPRESA BRASILEIRA DE SERVIÇOS HOSPITALARES -EBSERH
HOSPITAL DE DOENÇAS TROPICAIS DA UNIVERSIDADE FEDERAL DO TOCANTINS – HDT/UFT

ANEXOS

1. MODELO DE TERMO DE RESPONSABILIDADE –EQUIPAMENTOS

EBSERH
HOSPITAIS UNIVERSITÁRIOS FEDERAIS

HOSPITAL DE DOENÇAS TROPICAIS – UFT

TERMO DE RESPONSABILIDADE – EQUIPAMENTOS

Patrimônio nº **Data:** **até**

Equipamento:

( ) Notebook ( ) Netbook ( ) Filmadora ( ) Câmera Fotográfica

(X) Datashow ( ) Outros:_____

Acessórios:

CABO VGA, CABO DE FORÇA E ADAPTADOR.

Declaração

Declaro para fins de **RESPONSABILIDADE**, que recebi nesta data o equipamento acima citado em perfeitas condições de uso, para fins de:

_____

_____

, devendo zelar pela sua guarda, conservação e devolução.

Nome:

E-mail: **SIAPE:**

Setor: **Fone:**

Assinatura:

Data da Devolução:

É EXPRESSAMENTE PROIBIDO O REMANEJAMENTO DE QUALQUER MATERIAL CONSTANTE DESTE TERMO, SEM AUTORIZAÇÃO DO SGII

MINISTÉRIO DA EDUCAÇÃO
EMPRESA BRASILEIRA DE SERVIÇOS HOSPITALARES -EBSERH
HOSPITAL DE DOENÇAS TROPICAIS DA UNIVERSIDADE FEDERAL DO TOCANTINS – HDT/UFT

2. MODELO DE TERMO DE RESPONSABILIDADE

EBSERH
HOSPITAIS UNIVERSITÁRIOS FEDERAIS

HOSPITAL DE DOENÇAS TROPICAIS – UFT
TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, portador (a) da cédula de identidade n.º _____, expedida pelo _____, em _____ e inscrito no C.P.F. sob o n.º_____, e lotado o(a)_____deste Hospital de Doenças Tropicais, DECLARO , sob pena das sanções cabíveis nos termos da _____ (legislação vigente) que assumo a responsabilidade por:

I) tratar o(s) ativo(s) de informação como patrimônio do HDT/UFT;

II) utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do (Nome do órgão ou entidade);

Nestes termos,

Araguaína, _____
(data)

Assinatura e Nome do usuário e seu setor organizacional

Assinatura e Nome da autoridade responsável pela autorização do acesso

MINISTÉRIO DA EDUCAÇÃO
EMPRESA BRASILEIRA DE SERVIÇOS HOSPITALARES -EBSERH
HOSPITAL DE DOENÇAS TROPICAIS DA UNIVERSIDADE FEDERAL DO TOCANTINS – HDT/UFT

2. MODELO DE TERMO DE CIÊNCIA

EBSERH
HOSPITAIS UNIVERSITÁRIOS FEDERAIS

HOSPITAL DE DOENÇAS TROPICAIS – UFT

TERMO DE CIÊNCIA

Pelo presente, eu, _____, portador (a) da cédula de identidade n.º _____ e inscrito no C.P.F. sob o n.º _____, residente e domiciliado na_____, nº ____, na cidade de _____, estado do _____, declaro ter ciência da Política de Segurança da Informação (PSI), bem como suas normas complementares, comprometendo-me a cumprir o disposto no citado diploma.

Nestes termos,
Araguaína-TO, _____
(data)

Assinatura e Nome do usuário