

POLÍTICA DE SEGURANÇA EM TI

TECNOLOGIA DA INFORMAÇÃO

CONTROLE DE REVISÃO

Data	Revisão	Natureza da Alteração	Página revisadas
30/03/22	2	Objetivo	todas
30/03/22	2	Abrangência e Adesão	todas
30/03/22	2	Responsabilidade	todas
30/03/22	2	Tecnologia da informação	todas
30/03/22	2	Gestores	todas
30/03/22	2	Todos os níveis hierárquicos	todas
30/03/22	2	Documentos Complementares	todas
30/03/22	2	Finalidade dos Recursos Computacionais e Direito à Propriedade	todas
30/03/22	2	Descrição da Política Salvaguarda de Arquivos:	todas
30/03/22	2	Regras para utilização de contas e senhas da Rede Corporativa:	todas
30/03/22	2	Bloqueio USB e controle de acesso físico e lógico a unidades em nuvens:	todas
30/03/22	2	Acesso VPN (acesso remoto)	todas
30/03/22	2	Backups	todas
30/03/22	2	Data Center	todas
30/03/22	2	Procedimento de retirada de acesso	todas
30/03/22	2	Notebooks, Tablets (BYOD)	todas
30/03/22	2	Software e Computadores:	todas
30/03/22	2	Regras para utilização da Rede Corporativa	todas
30/03/22	2	Utilização do Correio Eletrônico (e-mail):	todas
30/03/22	2	Regras para utilização da Internet na Rede Corporativa do Hospital Santa Júlia	todas

	POLÍTICA DE SEGURANÇA EM TI
	TECNOLOGIA DA INFORMAÇÃO

Sumário

1 - Objetivo.....	1
2 - Abrangência e Adesão.....	1
3 - Responsabilidades.....	1
3.1 - Tecnologia da informação:.....	1
3.2 - Gestores:	1
3.3 - Todos os níveis hierárquicos:.....	2
4 - Documentos Complementares	2
5 - Finalidade dos Recursos Computacionais e Direito à Propriedade	2
5.1 - Regras de utilização do Recursos	2
6 - Descrição da Política	2
6.1 - Salvaguarda de Arquivos:.....	2
6.2 - Regras para utilização de contas e senhas da Rede Corporativa:	3
6.3 - Bloqueio USB e controle de acesso físico e lógico a unidades em nuvens:	3
6.4 - Acesso VPN (Acesso Remoto)	3
6.5 - Backups	3
6.6 - Data Center	3
6.7 - Procedimento de retirada de acesso	4
6.8 - Notebooks, Tablets (BYOD – Dispositivo Próprio)	4
6.9 - Software e Computadores	4
6.10 - Regras para utilização da Rede Corporativa	5
6.11 - Utilização do Correio Eletrônico (e-mail).....	5
6.12 - Regras para utilização da Internet na Rede Corporativa	6



POLÍTICA DE SEGURANÇA EM TI

TECNOLOGIA DA INFORMAÇÃO

1 - Objetivo

Estabelecer diretrizes que permitam aos colaboradores e prestadores de serviço do Hospital Santa Júlia seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da Instituição.

Preservar as informações do Hospital Santa Julia quanto à:

- **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.
- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

2 - Abrangência e Adesão

Esta Política abrange todos os colaboradores, bem como terceirizados que possuam acesso a informações confidenciais do Hospital Santa Júlia, dentro dos limites definidos, os colaboradores que concordarem com a política registrando o aceite através da assinatura do **TERMO DE COMPROMISSO DE TI** apresentado quando de sua admissão na empresa. Este termo determina a adesão do profissional a todas as políticas e normas internas, incluindo esta política. O uso indevido dos recursos, em desacordo com a política poderá implicar em advertência, suspensão e demissão a critério da direção da empresa, conforme previsto no item 7. dessa política.

3 - Responsabilidades

A Diretoria do Hospital Santa Júlia entende que o sistema de segurança adotado pelo Setor de Tecnologia da Informação somente atingirá sua eficácia com o comprometimento e a cooperação de TODOS os profissionais envolvidos nos processos: equipe de Tecnologia da Informação, Diretoria, Gestores e Colaboradores.

3.1 - Tecnologia da informação:

- 3.1.1 Definir e divulgar as medidas de Segurança da Informação;
- 3.1.2 Instalar ou remover componentes, fazer manutenção e controlar hardware e software;
- 3.1.3 Homologar hardware e software;
- 3.1.4 Autorizar tecnicamente a aquisição de hardware e software;
- 3.1.5 Realizar auditorias de hardware e software, com finalidade de garantir a proteção dos recursos computacionais e seu uso exclusivo nas atividades do hospital;
- 3.1.6 Adquirir serviços de informática

3.2 - Gestores:

- 3.2.1 Zelar pelo cumprimento destas normas e procedimentos e notificar imediatamente a TI sobre quaisquer vulnerabilidades e ameaças de quebra de segurança;
- 3.2.2 Educar os colaboradores sobre os princípios / procedimentos de Segurança da Informação, bem como lhes assegurar treinamento para o uso correto dos recursos, visando evitar falhas e danos ao funcionamento dos sistemas;
- 3.2.3 Solicitar à TI autorização para acesso do usuário aos sistemas de informação, bem como atualizar as solicitações de autorização sempre que houver alterações nos sistemas ou funções nas áreas de atuação;
- 3.2.4 Advertir formalmente o usuário e aplicar as sanções cabíveis quando este violar os princípios ou procedimentos de segurança, relatando imediatamente o fato à TI;
- 3.2.5 Antes de aprovar a solicitação de compra ou alteração de hardware e software, assegurar que o profissional responsável da TI foi consultado e efetuou a autorização técnica;

3.3 - Todos os níveis hierárquicos:

- 3.3.1 Responder pela guarda e proteção dos recursos computacionais colocados à sua disposição para o trabalho;
- 3.3.2 Responder pelo uso exclusivo e intransferível de suas senhas de acesso. Em caso de dúvidas, solicitar orientação à TI;
- 3.3.3 Adquirir conhecimento técnico necessário para a correta utilização dos recursos;
- 3.3.4 Relatar prontamente ao Gestor da TI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, vírus, acesso indevido ou desnecessário a pastas / diretórios de rede, acesso indevido à Internet, programas instalados sem conhecimento da TI etc.;
- 3.3.5 Não tentar obter acesso não autorizado a sistemas ou recursos da rede de computadores interna ou externamente;
- 3.3.6 Assegurar que as informações e dados de propriedade do Hospital Santa Júlia não sejam disponibilizados a terceiros, a não ser com autorização por escrito de um Diretor;
- 3.3.7 Relatar ao Gestor da TI ou um de seus colaboradores a possibilidade de instalação de um novo software ou aquisição de novo Hardware para a melhoria dos serviços prestados.

4 - Documentos Complementares

- Termo de Responsabilidade de equipamento particular;
- Política de Backup HSJ;
- Política de Firewall HSJ;
- Termo de Concessão de VPN.

5 - Finalidade dos Recursos Computacionais e Direito à Propriedade

Os recursos da Tecnologia de Informação disponibilizados pelo Hospital Santa Júlia são destinados exclusivamente às atividades da instituição. Os programas homologados e instalados nos computadores e nos servidores de rede são propriedade exclusiva do Hospital Santa Júlia, sendo vetada sua cópia parcial ou integral.

5.1 - Regras de utilização do Recursos

- 5.1.1 Não utilize os equipamentos de Informática e Telefonia para fins pessoais.
- 5.1.2 Uso da Internet somente é permitido para sites de interesses profissionais do Hospital.
- 5.1.3 Não compartilhe suas senhas e não as utilize de forma indevida.
- 5.1.4 Utilize os sistemas aos quais possui acesso com prudência e responsabilidade.
- 5.1.5 Não mantenha arquivos pessoais nos diretórios de rede ou computadores do Hospital ou utilize arquivos profissionais para fins pessoais.
- 5.1.6 Não utilize e-mail para fins pessoais ou assuntos considerados impróprios.
- 5.1.7 Ao se ausentar de sua estação de trabalho bloqueie imediatamente seu computador. É de responsabilidade de todos os colaboradores zelarem pelo patrimônio do Hospital, preservando e poupando as ferramentas e equipamentos de TI, utilizando-os somente para atividades profissionais relacionadas ao Hospital.

6 - Descrição da Política

6.1 - Salvaguarda de Arquivos:

- 6.2.1 Compete à TI criar e manter cópias de segurança (backups) dos dados de softwares críticos, armazenados nos servidores de redes;
- 6.2.2 Os usuários devem manter, obrigatoriamente, os dados críticos da empresa nos servidores de redes (file server);
- 6.2.3 São de responsabilidade exclusiva do usuário a cópia e a guarda dos dados gravados na estação local de trabalho;
- 6.2.4 Os backups devem ser guardados em local seguro, separados dos equipamentos, para viabilizar a recuperação dos dados.

6.2.5 Rotinas relacionadas aos backups se encontram no documento de Política de Backup HSI

6.2 - Regras para utilização de contas e senhas da Rede Corporativa:

- 6.2.1 Todos os usuários da Rede de Dados Corporativa do Hospital Santa Júlia receberão login e senha exclusivos para sua utilização e é obrigatório que todos os usuários tenham senhas individuais. É importante que os usuários não utilizem senhas de fácil identificação, tais como: data de nascimento próprio ou de parentes próximos, nomes próprios, datas comemorativas nacionais ou pessoais, iniciais de nomes próprios, números de telefones etc;
- 6.2.2 Não é permitida a utilização de computadores da rede sem senha ou com acesso local. Em caso de dúvidas, solicitar orientação à TI;
- 6.2.3 As contas e senhas são pessoais, os usuários deverão responder pelo uso exclusivo e intransferível de suas senhas de acesso, salvo nos casos em que as senhas são para acesso a computadores de uso coletivo (tal qual as recepções);
- 6.2.4 As senhas deverão ser trocadas pelo colaborador periodicamente;
- 6.2.5 Os usuários desligados terão suas contas bloqueadas imediatamente, assim como o acesso a qualquer recurso da rede.
- 6.2.6 Reserva-se ao Hospital Santa Júlia o direito de auditar a utilização de contas de rede fornecidas aos usuários de sua rede corporativa, sem se caracterizar invasão de privacidade.

6.3 - Bloqueio USB e controle de acesso físico e lógico a unidades em nuvens:

- 6.2.1 Por medida de segurança da informação são bloqueadas todas as portas USB e unidades de disco, drives A:\ removíveis como também unidade em nuvens como: Dropbox, SkyDrive, Google Drive, One Drive SugarSync e Amazon Cloud Drive etc. Unidades de CD, DVD dos computadores da empresa.

6.4 - Acesso VPN (Acesso Remoto)

- 6.2.2 O acesso a rede do Hospital Santa Júlia por meio da VPN é destinado a colaboradores ou prestadores de serviços que por alguma necessidade de interesse da empresa possam desenvolver suas atividades a distâncias, nenhum acesso é liberado sem aprovação do gestor do solicitante que deve ser assinado através do **Termo de Concessão de VPN**.

6.5 - Backups

- 6.2.3 A política de backup desenvolvida para o Hospital Santa Júlia tem como finalidade manter a integridade e a disponibilidade das informações e dos recursos de processamento necessários para o negócio do Hospital, a descrição de toda política se encontra no documento Política de Backup HSI.

6.6 - Data Center

- 6.6.1 O acesso ao Datacenter somente deverá ser feito por sistema forte de autenticação. Por exemplo: biometria, cartão magnético entre outros.
- 6.6.2 Todo acesso ao Datacenter, pelo sistema de autenticação forte, deverá ser registrado (usuário, data e hora) mediante software próprio.
- 6.6.3 Deverá ser executada semanalmente uma auditoria nos acessos ao Datacenter por meio do relatório do sistema de registro.
- 6.6.4 O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado, que deverá assinar um protocolo de visita que ficará dentro do datacenter.
- 6.6.5 O acesso ao Datacenter, por meio de chave, apenas poderá ocorrer em situações de emergência, quando a segurança física do Datacenter for comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando.
- 6.6.6 O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Serviços Gerais.
- 6.6.7 Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.
- 6.6.8 A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a autorização formal desse instrumento pelo responsável do Datacenter.

6.6.9 No caso de desligamento de empregados ou colaboradores que possuam acesso ao Datacenter, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação.

6.7 - Procedimento de retirada de acesso

- 6.7.1 Quando um colaborador é desligado do Hospital Santa Júlia, ele perde imediatamente o direito de acesso aos diversos ambientes de rede, serviço de e-mail externo e internet. Este procedimento é iniciado quando do envio de Check List de desligamento, quando as áreas responsáveis pelos acessos deverão providenciar o cancelamento das credenciais de acesso de profissional.
- 6.7.2 No caso de transferências internas, os direitos de acesso originais são retirados na data prevista no Check List de transferência. Os novos acessos seguem o perfil básico, sendo necessária a abertura de chamado para liberação dos demais acessos a sistemas e ambientes da rede necessários ao desenvolvimento das atividades na nova área. É possível que por um período pré-determinado, o profissional utilize informações e arquivos de ambas as áreas, em função da necessidade das áreas. Caso isso seja necessário, o profissional deve solicitar, através de abertura de chamado, a manutenção dos acessos antigos ou liberação dos novos acessos, com a justificativa sobre a manutenção de ambos os acessos, bem como o prazo máximo de manutenção deles, não podendo ultrapassar 30 dias.
- 6.7.3 Os profissionais demissionários terão, em caso de solicitação por parte de seu gestor imediato, os e-mails monitorados através de cópia das mensagens enviadas para a caixa postal do gestor, além de monitoramento semanal dos sites visitados pelo associado até o desligamento efetivo do profissional.
- 6.7.4 Os trabalhos desenvolvidos ou elaborados pelo Associado pertencem exclusivamente ao Hospital Santa Júlia, não cabendo ao associado o direito de retirá-lo ou copiá-lo quando de seu desligamento, não sendo permitida a gravação de arquivos em qualquer mídia sem a devida autorização por parte da TI Compliance.

6.8 - Notebooks, Tablets (BYOD – Dispositivo Próprio)

- 6.8.1 Equipamentos como notebook pessoal/terceirizado e tablet devem ter autorização expressa da diretoria através da assinatura do **TERMO DE RESPONSABILIDADE DE EQUIPAMENTOS PARTICULAR**, sendo seu uso proibido dentro da instituição sem a expressa autorização.

6.9 - Software e Computadores

- 6.9.1 Para mantermos o ambiente lógico, todos os softwares/aplicações operacionais devem ser homologados pelos usuários das áreas envolvidas, que devem verificar os impactos das novas versões nos procedimentos, resultados.
- 6.9.2 **Aquisição:** A aquisição de softwares ocorrerá conforme planejamento orçamentário, com base na homologação técnica por parte da equipe de TI, após validação das necessidades de uso pela diretoria da empresa.
- 6.9.3 **Instalação:** Somente a equipe de TI INFRA/SUORTE está autorizada a realizar instalação de qualquer tipo de software, seja este um sistema ou um aplicativo simples, principalmente aqueles obtidos gratuitamente e/ou baixados da internet.
- 6.9.4 **Licença de Uso:** Somente poderão ser instalados e utilizados softwares devidamente licenciados para uso do Hospital. Não é permitido instalar softwares pessoais, emprestados, de terceiros, que não sejam devidamente licenciados para uso do Hospital pelo fabricante do produto.
- 6.9.5 **Auditoria:** Poderá ser utilizada pela equipe de TI INFRA uma ferramenta automatizada para auditoria de softwares instalados nos computadores.
- 6.9.6 **Marcas e Modelos:** Utilização de equipamentos padronizados pela equipe de TI INFRA.
- 6.9.7 **Distribuição:** Os computadores são disponibilizados conforme necessidades de uso de cada
- 6.9.8 colaborador, com base nas atividades de suas áreas com prévia solicitação do gestor responsável do setor. As impressoras ficarão distribuídas em centros de impressão, localizados em pontos que melhor atendam a maioria dos colaboradores e não estejam em áreas que impliquem em risco à segurança das mesmas.

- 6.9.9 **Propriedade:** Os softwares, incluindo os desenvolvidos internamente, e recursos computacionais diversos pertencem exclusivamente ao Hospital Santa Júlia, bem como todos os direitos relativos a todas as invenções, inovações tecnológicas e criações intelectuais elaboradas e desenvolvidas pelos Colaboradores, Prestadores de Serviços e Consultores, durante a vigência da relação de emprego ou relação contratual.
- 6.9.10 É proibido a instalação de softwares piratas dentro da instituição, seja ele trial ou demo nos computadores da empresa, qualquer solicitação de softwares deve ser solicitada e justificada pelo gestor da área requisitante.
- 6.9.11 Serão instalados nos computadores somente softwares homologados pela TI. O uso de software não licenciado é crime previsto na Lei 9.609 de 19 de fevereiro de 1998. Além disso, existe um risco considerável na utilização de quaisquer softwares externos ao ambiente, destes possuírem vírus ou outras ameaças de segurança escondidas.

6.10 - Regras para utilização da Rede Corporativa

- 6.10.1 Todos os recursos de rede de computadores deverão ser utilizados exclusivamente para fins profissionais, que envolvam atividades relacionadas ao bom andamento dos serviços e processos do Hospital Santa Júlia.
- 6.10.2 Todos os arquivos que não tenham fins profissionais devem ser apagados dos equipamentos para evitar problemas futuros com auditorias;
- 6.10.3 Todos os computadores do Hospital Santa Júlia devem ter antivírus instalado e atualizado periodicamente. É proibido desinstalar e utilizar computadores sem antivírus instalado. Essa instalação é realizada pelos profissionais da TI;
- 6.10.4 É expressamente vedado aos usuários a instalação ou remoção de programas de computador, componente e periféricos;
- 6.10.5 É proibido aos usuários conectar celulares, tablets, smartphones ou computadores pessoais ou de terceiros à rede corporativa do Hospital Santa Júlia, salvo em casos expressamente autorizados pela Diretoria;
- 6.10.6 Para o acesso da rede por terceirizado ou prestadores de serviços com computador pessoal é necessário aprovação pela Diretoria **TERMO DE RESPONSABILIDADE DE EQUIPAMENTOS PARTICULAR.**

6.11 - Utilização do Correio Eletrônico (e-mail)

- 6.11.1 O Hospital Santa Júlia fornecerá, a seu critério, contas de correio eletrônico (@hospitalsantajulia.com.br) aos seus colaboradores. As Mensagens de correio eletrônico (e-mails) internos e externos devem ser exclusivamente de caráter profissional, sendo proibido qualquer tipo de utilização particular. O mesmo vale para arquivos anexos;
- 6.11.2 Todas as mensagens recebidas de origem desconhecida deverão ser eliminadas imediatamente, sem leitura de seu conteúdo, para evitar contaminação por vírus e outros riscos. Quaisquer tipos de comunicados e informativos corporativos deverão ser previamente aprovados e posteriormente divulgados pelo Qualidade e/ou Marketing;
- 6.11.3 É proibido configurar e/ou manter configuradas contas de correio eletrônico de servidores externos, isto é, diferentes de (@hospitalsantajulia.com.br), nos programas gerenciadores de correio eletrônico instalados em computadores da instituição. Em caso de dúvidas solicitar orientação à TI;
- 6.11.4 O correio eletrônico poderá ser utilizado a partir de qualquer computador conectado à Internet, utilizando-se o site de WebMail do Hospital Santa Júlia. Este site poderá ser acessado através do endereço <http://webmail.hospitalsantajulia.com.br>, ou através da Intranet do Hospital Santa Júlia, no endereço <http://santajulia/>
- 6.11.5 Este site de WebMail é o único com acesso permitido a partir de qualquer computador utilizando a rede do Hospital Santa Júlia. É proibido acessar contas de correio eletrônico de servidores externos através de sites de Webmail, salvo os autorizados pelo Gestor da área;
- 6.11.6 As caixas postais de contas de correio eletrônico do Hospital Santa Júlia (@hospitalsantajulia.com.br)

tem limite de tamanho de 10 Gb (Gigabytes)–e as mensagens enviadas/recebidas poderão conter arquivos anexos com até 5MB (5 Megabytes) por mensagem;

6.11.7 O conteúdo das mensagens enviadas através de contas de correio do Hospital Santa Júlia (@hospitalsantajulia.com.br) é de inteira responsabilidade do usuário que utiliza a conta e que possui a senha com acesso exclusivo à caixa postal e para envio de mensagens;

6.11.8 É proibida a utilização do e-mail para fins ilegais, transmissão de material de qualquer forma censurável, que viole direitos de terceiros e leis aplicáveis;

6.11.9 É proibida a utilização de e-mail para transmitir mensagens conhecidas como Spam, JunkMail, correntes ou a distribuição de mensagens em massa não solicitadas;

6.11.10 A troca da senha para acesso a caixas postais e envio de mensagens poderá ser efetuada através do site <http://webmail.hospitalsantajulia.com.br>. Em caso de dúvidas, solicitar orientação à TI;

6.11.11 É terminantemente proibido aos colaboradores da TI, administradores de rede e/ou correio eletrônico, ler mensagens de correio eletrônico de qualquer usuário quando estiver realizando serviços de manutenção e suporte, exceto quando em cumprimento de determinações da Diretoria do Hospital Santa Júlia para efeitos de auditoria.

6.11.12 Reserva-se ao Hospital Santa Júlia o direito de auditar a utilização de suas contas de correio eletrônico da instituição (@hospitalsantajulia.com.br) fornecidas aos usuários, sem se caracterizar invasão de privacidade.

6.12 - Regras para utilização da Internet na Rede Corporativa

6.12.1 O acesso à Internet é disponibilizado no Hospital Santa Júlia para viabilizar a busca de informações ou agilizar determinados processos da instituição.

6.12.2 Todo o acesso à Internet através da rede corporativa do Hospital Santa Júlia será controlado com a realização de auditorias nas páginas consultadas. Serão desenvolvidos relatórios com nomes, páginas consultadas e tempo de consulta. Estes relatórios serão enviados aos gerentes de cada área e à diretoria da instituição, para acompanhamento.

6.12.3 Os usuários são responsáveis por toda a utilização da Internet em computadores iniciados com seu login e senha. Quando o usuário se afastar do computador deverá encerrar a sessão através do “logoff”, reiniciar ou desligar o sistema.

6.12.4 É proibido aos usuários configurar ou alterar as configurações de rede e de acesso à Internet dos computadores do Hospital Santa Júlia, incluindo as seguintes configurações de rede:

6.12.5 IP, DNS, WINS, Gateway e Proxy. Em caso de dúvidas, solicitar orientação à TI;

6.12.6 Não é permitido enviar, baixar (download) ou manter arquivos de imagens, músicas, vídeo, arquivos executáveis em geral ou quaisquer outros de caráter pessoal;

6.12.7 É proibido o acesso a sites do gênero relacionamento, dos quais fazem parte: Facebook, Instagram, Google +, UOL, Gazzag, Meebo, etc. Salvo em casos autorizados pelo Gestor da Área e Gestor de TI.

6.12.8 Não é permitido o acesso a sites de Internet com conteúdo pornográfico, jogos, bate-papo, chat, blogger, cartoon, relacionamento, música, hacker ou que contenha ferramentas ou regras para invasões de rede, quebra de criptografia, senhas ou outros eventos de segurança;

6.12.9 É proibido o acesso a sites, a instalação e a utilização de programas de troca de mensagens instantâneas ou arquivos do tipo: Skype, Messenger, Bittorrent e outros, salvo em casos expressamente autorizados pelas respectivas Gerências Gerais.

6.12.10 As regras de acesso a internet, estão definidas e registradas no documento de Política de Firewall HSI.

	POLÍTICA DE SEGURANÇA EM TI
	TECNOLOGIA DA INFORMAÇÃO

ANEXO I – TERMO DE COMPROMISSO TI

Termo de Compromisso de acesso a TI do Hospital Santa Julia

Declaro que li e estou de acordo com a Política de Segurança da Tecnologia da Informação do Hospital Santa Julia, tendo ciência de todo o seu conteúdo. Declaro, ainda, estar ciente de que incidentes contrários à política de segurança resultarão em medidas que poderão chegar inclusive ao meu desligamento do quadro efetivo do Hospital Santa Julia, à quebra de contrato, aos processos judiciais ou a outras medidas pertinentes. Comprometo-me a preservar a integridade, a disponibilidade e a confidencialidade das informações obtidas durante a vigência do contrato com o Hospital Santa Julia, mesmo após o seu encerramento. Em sendo prestador de serviço terceirizado comprometo-me igualmente no cumprimento das regras e diretrizes previstas nesta PSTI.

Nome:

CPF:

Empresa: