POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Recife,15 de Junho de 2022

Versão 1

Sumário

1. Objetivo

Prover orientação e apoio relativo à segurança da informação e seus ativos (pessoas, sistemas, equipamentos, dados) da SPCC - Sociedade Pernambucana de Combate ao Câncer e de suas unidades sob gestão, sendo elas o Hospital da Mulher do Recife, UPAE Arruda, UPAE Arcoverde, UPAE Caruaru, UPAE Belo Jardim, Hospital São Sebastião, UPA Igarassu, para preservar sua integridade, disponibilidade e confidencialidade.

2. Abrangências

Esta política aplica-se a todos os colaboradores, prestadores de serviços, terceirizados e usuários de sistemas e serviços, seja de forma remota ou local ao ambiente de processamento de dados ou rede de computadores da SPCC.

3. Papéis e responsabilidades

3.1.1 Alta Gestão

Assegurar que a segurança da informação esteja integrada aos atuais processos da organização.

3.1.2. Responsável pela Segurança da Informação

A Segurança da Informação é responsabilidade de todos (usuários, colaboradores, prestadores de serviço, terceiros, etc.) que utilizam os recursos computacionais e redes de computadores da SPCC. Em caso de extravio, furto ou roubo o usuário deverá registrar boletim de ocorrência e comunicar imediatamente a T.I através do email: infra@hcp.org.br para HCP e informatica@hcpgestao.org.br para HCP Gestão, relatando o caso para que se proceda o cancelamento dos acessos e as medidas de segurança quanto ao equipamento. Em caso de incidentes, dúvidas,

sugestões ou orientações quanto à segurança da informação, acionar o setor de T.I nos ramais 8041 ou 8246 (HCP) e 142 (HCP Gestão).

3.1.3. Responsável pela Privacidade de Dados

O Encarregado de Dados (DPO) é a pessoa designada pela SPCC para atuar como elo de comunicação com a Autoridade Nacional de Privacidade de Dados (ANPD), com os titulares de dados e auxiliar no projeto de adequação a Lei Geral de Proteção de Dados (LGPD). Em caso de incidentes, dúvidas, sugestões ou orientações quanto à privacidade de dados pessoais ou dados pessoais sensíveis, acionar o DPO.

Nome: João Job | E-Mail: dpo@hcp.org.br | Telefone: (81) 98949 5260

3.1.4. Recursos Humanos

Comunicar e atualizar a T.I, imediatamente, sobre todas as informações referentes à movimentação de pessoal que tenham relação com a criação, alteração e desativação de usuários dos serviços de T.I.; Organizar treinamento em segurança da informação e de melhores práticas quanto ao uso de recursos de tecnologia; Providenciar a adesão a termos de confidencialidade, consentimentos, manuais de conduta e normas internas da SPCC de todos os novos colaboradores e/ou demais profissionais terceirizados.

3.1.5. Tecnologia da Informação

Desenvolver e adotar medidas de segurança, técnicas e administrativas, aptas para proteger os dados contra acessos não autorizados ou qualquer forma inadequada de acesso, com acompanhamento da área de Auditoria Interna; Seguir procedimentos que garantam à base tecnológica: Backups, segurança de dados, recuperação de desastres e continuidade de negócios da SPCC; Homologar novos recursos de tecnologia e segurança da informação; Criar processos que garantam a verificação de registros de atividades (“logs”) dos sistemas e recursos de tecnologia

de dados; Informar, registrar e tratar incidentes e requisições de tecnologia relacionados à segurança da informação e/ou continuidade do negócio.

4. Usuários de acesso aos sistemas e rede de computadores

Os acessos aos sistemas de informação, bancos de dados e a rede de computadores são administrados pelo setor de T.I. O acesso e uso dos sistemas de informação, diretórios de rede, bancos de dados e demais recursos devem ser restritos às pessoas, explicitamente autorizadas, e de acordo com a necessidade para o cumprimento de suas funções. Acessos desnecessários ou com privilégio excessivo serão imediatamente retirados. A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função. Cada usuário que utilizar os recursos de tecnologia da informação deve receber uma identificação exclusiva na rede, podendo variar entre os sistemas, mas nunca sendo usada por mais de um colaborador. Esta identificação deve obedecer a um padrão específico para cada sistema.

Padrão a ser adotado para login: [nome.ultimonome]. Em caso de já existir tal combinação, adotar nome.penultimonome. Em persistindo será adotado combinação com as iniciais do segundo nome nome.inicialdosegundonome+ultimonome. Periodicamente, os acessos serão revistos pelo T.I, como forma de controlar / revisar a pertinência dos acessos existentes. Contas de acesso ativas e sem atividades com mais de 45 dias serão automaticamente bloqueadas e sem aviso prévio.

4.1. Do cadastro, ativação de usuários

O tempo para atendimento de chamado (SLA) para criação de usuários de acesso pela T.I é de até 48hrs (2 dias úteis). Todas as admissões, demissões, promoções, transferências de departamento e/ou unidade, contratos com terceiros, o departamento de Recursos Humanos (RH) deverá registrar um chamado na T.I, descrevendo o setor, função, gestor imediato, nome completo, ID funcional e se faz ou fará uso de recursos corporativos como e-mail e smartphone. Não deve ser

informado dados pessoais ou sensíveis, além das informações acima descritas, ou que não serão aplicadas para o determinado fim de acesso. Para o caso de novos colaboradores ou prestadores de serviços, os acessos e os termos de responsabilidades e confidencialidade serão entregues durante o processo de integração previamente agendado pelo RH. Para os casos de acessos temporários (consultores, estagiários, terceiros, jovem aprendiz, ou similares) deverá estar descrito no chamado o período de acesso inicial e final. Ao chegar na data fim de validade do usuário em não havendo comunicação prévia de 48hrs (2 dias úteis) o acesso será automaticamente expirado. Sendo necessário nova abertura de chamado para reativação. Não será atendido qualquer movimentação de pessoal que não tenha abertura de chamado para a T.I com origem RH. Cabe ao setor de RH dar conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação à Política de Segurança da Informação da SPCC (Anexo VI). Nenhum colaborador, estagiário, temporário, terceiro ou prestador de serviço poderá ser contratado, sem ter expressamente concordado com esta política. Os contratos com as empresas prestadoras de serviços que possuem acesso às informações, aos sistemas e/ou ambiente de rede da SPCC devem conter cláusulas que assegurem o cumprimento das regras de segurança da informação e privacidade de dados e suas penalidades no caso de descumprimento. Bem como, deverá conter de forma clara e objetiva quanto ao uso de equipamentos e recursos de softwares a serem cedidos pela SPCC para realização de suas atividades no período contratado. Não é de responsabilidade da T.I, manutenção, atualização, aquisição e suporte em computadores, notebooks, impressoras ou equipamentos que NÃO sejam de propriedade da SPCC. Com exceção daqueles equipamentos que façam parte de contratos ativos (aluguel de equipamentos), que é de responsabilidade da TI controlar, monitorar e assegurar o suporte em tempo hábil. É terminantemente proibido a instalação de softwares e recursos da SPCC em equipamentos pessoais ou de terceiros.

5. Desativação de usuários

Para os casos de demissão as demandas serão atendidas em até 2hrs após registro do chamado. Cabe ao RH registrar chamado no sistema de service desk solicitando a desativação de usuários por demissões, mudanças de funções ou fim de contratos com terceiros para que a T.I realize os devidos ajustes ou desativação do perfil de acesso. Cabe ao RH realizar check list demissional junto ao colaborador para certificar das desativações de acesso, retenção de equipamentos (celular, chip, notebook, tablets, etc.) que estão sob responsabilidade do usuário.

6. Da Segurança de Dados

Os controles de acesso lógico são implantados com o objetivo de garantir que apenas usuários autorizados tenham acesso aos recursos necessários para execução de suas tarefas; e os usuários estejam impedidos de executar transações incompatíveis com sua função ou além de suas responsabilidades.

6.1. Política de Senha

A senha inicial de acesso a rede de computadores e sistemas são temporárias em procedimento de cadastro no setor de TI, a qual deve ser alterada obrigatoriamente no primeiro acesso pelo usuário. As seguintes diretivas de conta de acesso são aplicadas:

- Não é permitido a utilização das últimas 3 (três) senhas de acessos;
- Será solicitado automaticamente a alteração da senha a cada 60 dias;
- A senha de acesso deverá atender requisitos mínimos de complexidade. Tamanho mínimo 8 caracteres, utilização de letras, números e caracteres especiais (por exemplo, !, $, #, %);
- A conta de acesso será bloqueada automaticamente após 5 (cinco) tentativas de acesso inválidas. Após bloqueio, o sistema liberará automaticamente para nova tentativa após 10 minutos;

- Não é possível a recuperação da senha, apenas a sua redefinição via chamado para T.I.;
- Bloqueio para acesso aos sistemas de gestão utilizando dois computadores de maneira simultânea com mesmo login de acesso;
- Não será exibido o nome do último usuário que fez login, sendo necessário a digitação de usuário e senha para cada novo logon de acesso.

As contas de usuários com suas respectivas senhas são únicas, pessoais e não compartilhadas de forma a possibilitar a identificação dos autores de atividades realizadas nos sistemas. Os usuários deverão manter sua senha em total sigilo e são responsáveis por proteger as informações às quais possuem acesso. A violação da confidencialidade pode acarretar responsabilidades legais, além de expor informações confidenciais da SPCC. Não é permitido manter as senhas registradas em arquivos na rede, no computador, em lembretes ou qualquer outro tipo de anotação. Não é recomendado que o usuário utilize senhas fracas em nenhum recurso computacional. Entende-se por senhas fracas, nomes, palavras de dicionário, datas, placas de veículos, dígitos sequenciais do teclado, padrões, entre outros. Esses tipos de senhas são facilmente descobertos por softwares específicos para este fim.

6.2. Proteção de tela

Automaticamente após 7 minutos de inatividade a tela do equipamento esmaecerá e após 15 minutos de inatividade a sessão do equipamento será bloqueada e solicitada nova autenticação (nome do usuário e senha). Para as áreas assistenciais, como emergência, urgência, recepção, ambulatórios, consultórios, triagem, automaticamente após 15 minutos de inatividade a tela do equipamento esmaecerá e após 30 minutos de inatividade a sessão do equipamento será bloqueada e solicitada nova autenticação (nome do usuário e senha). Com esta medida o objetivo é evitar que pessoas não autorizadas tenham acesso a dados confidenciais, pessoais ou sensíveis, seja de forma visual ou por manipulação dos sistemas.

6.3. Tratamento de Mídias (USB, Pen drive, Bluetooth)

A utilização de mídias removíveis (portáteis) de armazenamento, pen drives, hds externos, cartões de memória e similares são uma provável fonte para infecção da rede de computadores por malwares, virus, worms, adware, spyware, ransomware, bots, rootkit ou qualquer outra ameaça maliciosa que possa ser transmitida por mídias digitais. Além de possibilitar evasão de dados e informações corporativas para além do controle da SPCC. As portas de comunicação USB e barramentos similares como bluetooth são automaticamente bloqueadas por software de gerenciamento central. Para concessão de acesso será necessário o registro de chamado para T.I, anexando o termo de autorização específico para tal responsabilidade (Anexo I). Este termo tem por objetivo atribuir responsabilidade ao usuário solicitante do acesso, que concorda expressamente, juntamente com seu gestor imediato, que é de sua inteira, exclusiva e total responsabilidade por manter a integridade, confidencialidade e disponibilidades dos dados e equipamentos da SPCC para uso com mídias removíveis conectadas a USB ou qualquer outro tipo de barramento.

Esta concessão de acesso tem prazo de validade de 90 dias a partir da data constante no termo de responsabilidade.

7. Licenças de Softwares

Os softwares instalados nos equipamentos corporativos devem atender à Lei nº 9.609/98 (Lei de Software) e Lei nº 9.609/98 (Lei dos Direitos Autorais), assim, nenhum software deve ser instalado sem o devido licenciamento ou sem prévia autorização do Depto. de T.I. Nenhum colaborador, estagiário, terceiro, prestador de serviço, usuário ou similar possui autorização para copiar ou ceder software da empresa à terceiros ou instalar software não regular, ficando sujeito à rescisão de contrato, assim como à responsabilidade pessoal por tais atos; Periodicamente é realizado pelo Departamento de T.I inventário de software para constatar e verificar a existência de softwares não regulares que, caso existam, implicará na remoção imediata e sem aviso prévio.

8. Do Acesso Remoto

8.1. Aplicativos de assistência remota

O uso de aplicativos ou softwares para assistência remota como Anydesk, TeamViewer, Remote Desktop, ou similares não são permitidos, sendo bloqueado automaticamente por software de gerenciamento central. Assim como a maioria dos softwares requerem licenças de uso. Em casos de ser necessário para prestação de assistência técnica por prestadores de serviços, com o devido contrato de serviço ativo, deverá ser aberto chamado no sistema da T.I para concessão temporária, exclusiva e com acompanhamento técnico da T.I.

8.2. Do Uso da VPN (Conexão Remota)

Nos casos em que for requerida a utilização de conexão remota por VPN à rede da SPCC será necessário o preenchimento e assinatura do Gestor no Termo de Responsabilidade de Uso da VPN (Anexo II) devendo ser anexado ao chamado. O usuário declara conhecer, compreender e concordar expressamente com o presente Termo de Uso, e cumprir com todas as suas condições. São responsabilidades do usuário do serviço de VPN:

A. O usuário deverá garantir que o acesso remoto à rede da SPCC não seja utilizado por pessoas não autorizadas. Os dados fornecidos para acesso são pessoais e intransferíveis.

B. Os direitos de acesso serão liberados por demanda a T.I e no prazo de validade de 30 dias. Renováveis mediante assinatura de novo Termo.

C. O acesso à rede da SPCC não deverá ser utilizado a partir de equipamentos de uso público (cyber cafés, business centers, wi-fi públicas etc.)

D. Efetuar e manter a correta configuração do sistema operacional, dos softwares e demais componentes que componham a solução, contando com o suporte técnico da T.I.

E. Para os casos excepcionais, onde o equipamento a ser utilizado não seja da SPCC, problemas gerais do computador não estão cobertos por esse suporte.

F. Tratar qualquer incidente de segurança que venha ser identificado com urgência e prioridade adequados, evitando toda e qualquer forma de postergação.

G. O usuário será responsável por quaisquer incidentes de segurança gerados ativa ou passivamente pelo(s) equipamento(s) utilizado(s) para realizar a conexão remota à rede.

H. Tomar as medidas necessárias em decorrência de manutenções programadas e comunicadas pela T.I.

I. Não ceder, informar, emprestar, passar e/ ou o que o valha, a chave de acesso da VPN para terceiros em hipótese alguma;

J. Usar o software e as informações obtidas única e exclusivamente para a finalidade determinada;

K. Permanecer fisicamente junto ao equipamento utilizado até que este seja desativado ou bloqueada a sessão;

L. Assegurar que nenhum relatório, tela ou listagem solicitado seja disponível sem sua presença e/ ou autorização;

M. Caso a utilização do acesso remoto resulte em transtorno para a estrutura da rede interna da SPCC, o direito de acesso remoto será suspenso imediatamente e sem aviso prévio.

N. Ao fazer uso da VPN, o usuário concorda e autoriza, expressamente, o monitoramento das suas interfaces de rede.

O. A T.I poderá monitorar as interfaces de rede para certificar a conformidade com este termo de serviço, sendo vedado ao usuário bloquear ou interferir no monitoramento, sem prejuízo do uso de tecnologias de criptografia e firewalls para ajudar a proteger seu conteúdo. A T.I, ao encontrar ou ser informado sobre indícios de violação dos termos de uso estipulados nesse documento, emitirá notificação ao Gestor do Usuário, podendo seu acesso ser suspenso até entendimento e/ou atendimento das orientações da T.I.

P. 8.3. Home Office (Trabalho Remoto)

Q. Nos casos de liberação para home office a solicitação deverá ocorrer via chamado ao T.I pelo departamento de RH, informando o nome, login de acesso do usuário, data de início, data fim da vigência da concessão de acesso e

anexar o Termo de Responsabilidade de Uso da VPN (Anexo II) devidamente assinado. Os equipamentos a serem utilizados devem ser de propriedade da SPCC respeitando os pré-requisitos de segurança de dados, assim como os de boas práticas de segurança como antivírus licenciado e atualizado, e sistema operacional original e atualizado.

9. Do uso das Impressoras e Scanners

As impressoras e scanners da SPCC deverão ser utilizados única e exclusivamente para atender às necessidades do negócio. Não devendo ser utilizados para fins particulares ou aqueles que se desviem das atribuições específicas da SPCC.

O conteúdo impresso e escaneado poderá ser monitorado, sendo possível a identificação do usuário, equipamento e material impresso.

O uso de scanners deve exclusivamente atender a demandas específicas e necessárias da instituição.

É terminantemente proibido a utilização das funcionalidades de scan e cópia para materiais que possuam Direitos autorais, uso de marcas.

Ao enviar documentos para impressão certifique-se de ter encaminhado para o local correto e que a impressão esteja segura para evitar o vazamento de informações e dados confidenciais, pessoais ou sensíveis.

10. Do uso da Internet

O acesso à internet é permitido, encorajado e autorizado para os usuários que necessitarem para o desempenho das suas atividades profissionais.

Os sites com informações que não tenham finalidade profissional ao negócio não devem ser acessados, uma vez que na internet há o perfil de acesso dos usuários

para navegação de sites com monitoramento periódico pelos sistemas de T.I como medida preventiva e otimização do uso do recurso.

Não é permitido instalar programas provenientes da Internet nos recursos de tecnologia da SPCC, sem expressa autorização do departamento da T.I, exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais.

Por questões de segurança alguns sites, serviços ou aplicativos podem ser bloqueados proativamente pelo firewall ou antivírus e caso o usuário/departamento necessite de acesso ao conteúdo bloqueado, deverá solicitar ao departamento de T.I via chamado, para análise da T.I e se for o caso solicitação de aprovação formal da sua gerência para liberação do acesso.

É de responsabilidade do departamento de cada usuário: a forma como a internet está sendo utilizada, os sites acessados e as informações nas quais o usuário transita. Qualquer acesso à internet criado fora das especificações desta diretriz, assim como qualquer violação, compartilhamento ou perda de informações da SPCC advinda do acesso indevido, também será de responsabilidade do setor.

É proibido os acessos a sites cujo conteúdo não seja de real utilidade aos negócios ou que violem as legislações vigentes. Por exemplo: sites de cunho racista ou discriminatório, erótico/ pornográfico, salas de bate papo, que incentivam práticas ilegais, pirataria de software etc.

É proibido efetuar cópias (download) na internet de softwares, assim como materiais gráficos, logomarcas, documentos ou outros que possam caracterizar pirataria ou violação de direitos autorais.

Quando o usuário não cumprir os critérios definidos nesta diretriz, o departamento de T.I poderá cancelar o acesso à internet, sem prévio aviso ao usuário. O departamento do T.I deve comunicar formalmente à gerência do departamento envolvido e ao departamento de Recursos Humanos, informando o motivo do cancelamento, devendo a gerência da área analisar o ocorrido e tomar as ações cabíveis.

O cancelamento também poderá ser solicitado formalmente pela gerência ou superintendência da área requisitante.

11. Do uso do e-mail

O uso do e-mail é individual e o usuário é responsável por toda mensagem enviada a partir de seu endereço.

As mensagens devem ser escritas em linguagem profissional e devem zelar pela imagem da SPCC.

É proibido o uso do e-mail que contenham declarações difamatórias, linguagem ofensiva, ideologias políticas, religiosas, raciais, pornográficas, apologia às drogas ou que possam prejudicar a imagem da organização, pacientes, concorrentes, fornecedores e que sejam incoerentes com as políticas da SPCC.

Não compartilhe dados pessoais e dados sensíveis através do e-mail. Caso sua atividade demande tal ação, certifique-se de que as pessoas destinadas e em cópia sigam a Política de Privacidade de Dados atendendo a Lei Geral de Proteção de Dados - LGPD (Nº 13.709/2018).

11.1. Corporativo

O e-mail corporativo fornecido pela SPCC é um instrumento de comunicação para a realização das atividades dos colaboradores autorizados e não poderá ser utilizado para fins pessoais ou para o fim que infrinja o Código de Ética da instituição. O colaborador deve prezar pela boa e responsável utilização de sua conta de e-mail corporativo.

O uso do e-mail da SPCC é um recurso que pode ser retirado a qualquer momento e sem aviso prévio quando constatado sua não utilização por um prazo igual ou superior a 60 (sessenta) dias ou quando caracterizada a utilização indevida e/ou abusiva. A discrição e discernimento próprios devem ser utilizados ao se enviar um e-mail.

Os usuários autorizados devem proteger o seu acesso ao sistema de e-mail da SPCC contra o uso desautorizado. Evite a utilização de sua conta em equipamentos públicos, redes abertas ou que representem risco à segurança da sua caixa postal.

Delete e-mails suspeitos sem abri-los. É extremamente recomendado aos usuários que verifiquem o conteúdo das mensagens recebidas e não cliquem em links suspeitos que possam gerar danos ao equipamento, ambiente corporativo ou que possam capturar informações relevantes da SPCC.

Para incluir um novo usuário no correio eletrônico, a respectiva gerência ou RH deverá fazer a solicitação formal, através de abertura de chamado ao setor de T.I. A T.I por sua vez deverá requisitar a contratação/compra ou realocação da licença para inclusão do colaborador indicado ao serviço de correio eletrônico

Os e-mails armazenados ou transferidos pelo sistema de e-mail da SPCC são de propriedade da SPCC. Assim, todos os e-mails recebidos ou enviados por e-mail corporativo estão sujeitos ao monitoramento integral do seu conteúdo pelos departamentos competentes, que poderão utilizar ou compartilhar tais informações de forma a atender a finalidade e necessidade específica da SPCC.

É restrito o acesso aos e-mails armazenados em caixas postais dos colaboradores, ativos, demitidos ou afastados. Somente a Gerência imediata está autorizada a avaliar e aprovar as solicitações de acesso a esta informação. O solicitante deve obter a aprovação formal da Superintendência Geral de Controladoria e via chamado, solicitar ao departamento de T.I este acesso.

Os usuários autorizados devem compor e-mails com o conhecimento de que se trata de um documento oficial que poderá ser lido pela SPCC e se tornar público.

A SPCC reserva o direito de acesso, auditoria, revisão, deleção, monitoração, revelação ou uso de todos os e-mails corporativos e outras informações armazenadas e transferidas no seu sistema de e-mail a qualquer momento e sem notificação prévia.

Usuários autorizados devem reportar qualquer violação ocorrida deste procedimento ao seu gestor ou aos Departamentos de T.I e Recursos Humanos. O que avaliar ser mais apropriado.

Todo conteúdo do e-mail, é de propriedade da SPCC, os usuários não devem esvaziar a caixa de e-mail ou eliminar arquivos dos sistemas internos em caso de ter seu contrato de trabalho suspenso ou finalizado.

11.2. Pessoal

A utilização pessoal em caráter limitada e ocasional do e-mail pessoal é permitida, desde que não interfira na produtividade dos colaboradores nem no desempenho das suas funções.

Não utilize o e-mail pessoal para tratar de temas referentes a SPCC. Sejam dados corporativos, pessoais ou sensíveis.

Não utilize recursos como drives virtuais (Dropbox, GoogleDrive, OneDrive e similares) para armazenar dados corporativos.

Não utilize recursos de compartilhamento de arquivos (Office365, Google e similares) para assuntos relacionados às atividades da SPCC.

12. Do uso do Wi-fi

12.1. Acesso Corporativo

O acesso a rede wi-fi corporativa está liberado exclusivamente para equipamentos de propriedade da SPCC com suas respectivas licenças de uso, antivírus e sistema operaciona atualizado e com suporte válido pelo fabricante e com chave de acesso exclusivo a ser fornecido e inserido pelo Departamento de T.I.

É terminantemente proibido o compartilhamento da chave de acesso da rede wi-fi corporativa por qualquer usuário, sendo responsabilidade do Departamento de T.I a troca periódica da chave de acesso a cada 60 dias.

Os filtros web, controle de aplicações, portas de acesso, prevenção de perda de dados, sistema de prevenção de intrusão (IPS) e perfis de acesso por grupo deverão ser os mesmos aplicados na rede cabeada.

12.2. Acesso visitante

O acesso Wi-fi visitante é uma cortesia oferecida pela SPCC mediante o aceite do Termo de Uso (Anexo III) disponibilizado no portal de autenticação (conexão) a rede wi-fi.

O serviço de wi-fi visitante poderá ser bloqueado, suspenso ou encerrado a qualquer momento por motivos técnicos ou administrativos a qualquer momento e sem aviso prévio.

A chave de acesso (voucher) será fornecida pelo Departamento de T.I mediante abertura de chamado. Com validade de 25 dias.

Alguns sites e serviços estão bloqueados com o objetivo de garantir a integridade, segurança, zelar pelo bom uso do recurso ou por estarem em não conformidade com as políticas da SPCC.

13. Do uso de equipamentos de terceiros na rede da SPCC

É terminantemente proibido a conexão de equipamentos de terceiros à rede da SPCC sem a prévia autorização do Departamento de T.I e mediante assinatura do Termo de Confidencialidade e Política de Segurança da Informação.

Se houver a necessidade de conectar os equipamentos de terceiros à rede de computadores, o mesmo deverá ter seu sistema operacional e antivírus licenciado e atualizado. Serão conectados à rede virtual para visitantes, sem acesso aos recursos corporativos, datacenter ou afins.

Em casos onde se faça necessário liberações técnicas para os recursos corporativos deverá ser registrado chamado para avaliação da T.I.

14. Do uso das redes sociais.

O acesso às redes sociais dentro da rede da SPCC está disponível para os departamentos e ou usuários que necessitem para realização de suas atividades operacionais. Só será liberado acesso a estes conteúdos, em extrema instância e mediante aprovação do Gestor imediato, onde deverá ser justificado pelo Gestor formalmente a real necessidade e o relacionamento com as funções do usuário.

Deverá ser solicitado este acesso com abertura de chamado ao departamento de T.I com as aprovações e justificativas necessárias anexadas.

A SPCC não se responsabiliza pelas políticas e práticas de coleta, uso e divulgação (incluindo práticas de proteção de dados) de outras organizações, incluindo todos os Dados Pessoais que divulgar para outras organizações por meio dos aplicativos ou páginas em mídias sociais.

É recomendado que o usuário se informe sobre a política de privacidade de cada site, aplicativo ou prestador de serviço utilizado.

14.1. Whatsapp e similares.

O uso do Whatsapp e aplicativos similares de mensagens fazem parte da rotina profissional e pessoal, no entanto, ao inserir na rotina profissional, algumas medidas preventivas quanto a segurança e privacidade de dados são necessárias.

O uso de dispositivos móveis pessoais não é recomendado para tratar de temas corporativos, dados pessoais e dados pessoais sensíveis pelo fato de que a SPCC não terá poder de decisão sobre o tratamento de dados pessoais no referido dispositivo.

Sugerimos que os smartphones ou dispositivos similares utilizem: antivírus licenciado e atualizado, sistemas operacionais (Android, IOs e demais) sempre atualizados, adotem senhas seguras (8 caracteres alfanuméricos), não utilizem padrões de desbloqueio de tela, ative o bloqueio de tela automático com tempo de duração mínimo, mantenha os aplicativos atualizados, remova os aplicativos que não

utiliza mais, habilite autenticação de dois fatores para todos os aplicativos que forem possíveis, não utilize wi-fi aberto (público), não utilize carregadores USBs públicos, ative a criptografia de seu dispositivo.

Em caso de perda ou roubo de seus smartphones ou dispositivos similares, se houver neles dados pessoais pertencentes ou relacionados à SPCC, comunique imediatamente ao DPO (dpo@hcp.org.br) informando os tipos de dados vazados e os impactos à SPCC.

Evite utilizar o aplicativo para compartilhar dados pessoais, dados pessoais sensíveis (exames, laudos, imagens) ou conteúdo estratégico da organização. Caso seja necessário, adote o envio de mensagens temporárias ou o procedimento de eliminar o mais breve possível de seu dispositivo após inserir o que for necessário nos sistemas de gestão da organização para minimizar o impacto em caso de vazamento. Realize este procedimento em até 24hrs. O compartilhamento de conteúdo de dados pessoais e dados pessoais sensíveis referentes a SPCC implica em corresponsabilidade jurídica sobre o dado.

Todos os exames e laudos devem estar registrados nos sistemas de gestão da SPCC.

Quanto aos grupos de Whatsapp e similares é recomendável que os administradores adotem algumas atitudes, como:

- Criar regras claras e objetivas sobre o tema do grupo e assuntos proibidos: Adicionar as regras à descrição do grupo. Deixar explícito que não serão admitidos racismo, ofensas, ou qualquer forma de intolerância e demais pontos pertinentes, sob pena de exclusão;
- Entrada de novos membros: Recomendar que a pessoa faça a opção de entrar no grupo por livre vontade, por meio de um link enviado a ela, e possa sair quando quiser. Após a entrada de cada convidado, redefina o link de convite;
- Monitorar o que acontece no grupo: Orientar os membros imediatamente caso iniciem uma discussão sobre algum tema fora do aceitável ou tenham um comportamento inadequado;

- Avalie selecionar alguns membros para dividir a responsabilidade da administração e ajudar a tomar decisões;
- Ajuste as configurações para que somente o administrador possa mudar o nome, imagem e a descrição do grupo, bem como desativar as mensagens temporárias;
- Faça o backup das mensagens do grupo com frequência, caso seja necessário usá-las como prova em um processo judicial.

15. Gestão de Ativo

Considera-se como ativo de TI os sistemas, computadores, notebooks, servidores, telefones fixos, linhas móveis e equipamentos de rede.

É de responsabilidade da TI manter inventário periódico e atualizado sobre os ativos de sua responsabilidade. Inclusive de definir os ciclos de vida e propor as renovações e ou melhorias necessárias para a Superintendência Geral.

Para comprar, substituição ou desenvolvimento de programas (software) ou equipamentos de informática (hardware) deverá ser solicitado via chamado para o departamento de TI para abertura do processo de homologação técnica. É necessário aprovação do Gestor imediato e da Superintendência responsável pela área antes de ser submetido para homologação ao TI. Não é permitido a homologação de qualquer sistema informatizado diretamente pelo usuário ou área final.

A disponibilização de Smartphones por parte da TI ocorrerá somente em caso de disponibilidade de equipamento. Em não tendo a disponibilidade a área demandante deverá providenciar junto a sua respectiva Superintendência a aprovação financeira para aquisição.

Os usuários que fizerem uso de notebooks e smartphones fornecidos pela SPCC deverão assinar o respectivo termo de responsabilidade (Anexo IV e V).

16. Auditoria dos computadores (Logs).

Os computadores, notebooks e servidores devem estar configurados para possibilitar a auditoria através dos logs de sistemas, segurança e aplicativos.

A análise desses logs será realizada em caso de suspeitas quanto a acessos não autorizados ou para dirimir outros tipos de dúvidas que possam surgir sobre a utilização dos equipamentos.

Deverão seguir as seguintes configurações aplicadas por política de grupo de domínio:

- Auditoria de acesso a objetos (êxito e falha);
- Auditoria de acesso ao serviço de diretório (êxito e falha);
- Auditoria de acompanhamento de processos (êxito e falha);
- Auditoria de alteração de políticas (êxito e falha);
- Auditoria de eventos de logon (êxito e falha);
- Auditoria de eventos de logon de conta (êxito e falha);
- Auditoria de eventos de sistema (êxito e falha);
- Auditoria de gerenciamento de conta (êxito e falha);
- Auditoria de uso de privilégios (êxito e falha).

Os arquivos de log deverão estar configurados para o tamanho de 30.464kb e para sobrescrever os eventos mais antigos primeiro.

17. Processo disciplinar em caso de violação da política

Nos casos em que ocorrer a violação desta política de segurança o Departamento de TI notificará imediatamente o Gestor responsável da área e o Departamento de Recursos Humanos para as devidas providências administrativas.

ANEXO I:

TERMO DE RESPONSABILIDADE PARA USO DE ARMAZENAMENTOS REMOVÍVEIS CONECTADOS A USB

O uso de armazenamentos removíveis é uma provável fonte para infecção da rede de computadores por malwares, virus, worms, adware, spyware, ransomware, bots, rootkit ou qualquer outra ameaça maliciosa que possa ser transmitida por mídias digitais. Além de possibilitar que dados e informações corporativas se propaguem para além da rede privada da SPCC.

Este termo tem por objetivo atribuir responsabilidade ao usuário abaixo descrito que concorda expressamente, juntamente com seu gestor imediato, que é de sua responsabilidade manter a segurança, integridade e sigilo dos dados e informações contidas no dispositivo removível e do equipamento por ele utilizado para conexão e acesso ao dispositivo de armazenamento removível seja USB ou barramentos similares.

As portas de comunicação USB e barramentos similares são automaticamente bloqueadas por software de gerenciamento central. Com a concordância deste termo o acesso será liberado para a estação solicitada.

Declaro estar ciente que é de minha inteira, exclusiva e total responsabilidade por manter a integridade, confidencialidade e disponibilidades dos dados e equipamentos da SPCC para uso com mídias removíveis conectadas a USB ou qualquer outro tipo de barramento.

Esta concessão de acesso tem prazo de validade de 90 dias a partir da data abaixo.

Recife, / /2022.

_____ _____

Nome: Nome:

Matrícula: Gestor

ANEXO II:

TERMO DE RESPONSABILIDADE PARA USO DE VPN

Através da assinatura deste documento, ... (usuário), me comprometo a seguir as normas descritas na PSI - Política de Segurança da Informação, por mim assinada, a partir da data, .../...../....., acessar remotamente os recursos da rede da SPCC

Declaro estar ciente das responsabilidades, abaixo descritas, e de acordo com a PSI:

1. É responsabilidade do usuário garantir que o acesso remoto à rede da SPCC não seja utilizado por pessoas não autorizadas. Os dados fornecidos para acesso são pessoais e intransferíveis.

2. Os direitos de acesso serão liberados por demanda a T.I e no prazo de 30 dias. Renováveis mediante assinatura de novo Termo.

3. O acesso à rede da SPCC não deverá ser utilizado a partir de equipamentos de uso público (cyber cafés, business centers, wi-fi públicas etc.).

4. Efetuar e manter a correta configuração do sistema operacional, dos softwares e demais componentes que componham a solução, contando com o suporte técnico da T.I.

5. Para os casos excepcionais, onde o equipamento a ser utilizado não seja da SPCC, problemas gerais do computador não estão cobertos por esse suporte.

6. Tratar qualquer incidente de segurança que venha ser identificado com urgência e prioridade adequados, evitando toda e qualquer forma de postergação.

7. O usuário será responsável por quaisquer incidentes de segurança gerados ativa ou passivamente pelo(s) equipamento(s) utilizado(s) para realizar a conexão remota à rede.

8. Tomar as medidas necessárias em decorrência de manutenções programadas e comunicadas pela T.I.

9. Não ceder, informar, emprestar, passar e/ ou o que o valha, a chave de acesso da VPN para terceiros em hipótese alguma;

10.Usar o software e as informações obtidas única e exclusivamente para a finalidade determinada;

11. Permanecer fisicamente junto ao equipamento utilizado até que o mesmo seja desativado ou seja bloqueada a sessão;

12.Assegurar que nenhum relatório, tela ou listagem solicitado seja disponível sem sua presença e/ ou autorização;

13.Caso a utilização do acesso remoto resulte em transtorno para a estrutura da rede interna da SPCC, o direito de acesso remoto será suspenso imediatamente e sem aviso prévio.

14.Ao fazer uso da VPN, o usuário concorda e autoriza, expressamente, o monitoramento das suas interfaces de rede.

_____

Informar a área de acesso/ computador/ servidor

_____

Justificativa

_____

Nome do Responsável, e-mail, telefone e assinatura

ANEXO III:

TERMO DE USO PARA REDE WI-FI VISITANTE

Ao acessar o Wi-fi (rede sem fio) visitante da Sociedade Pernambucana de Combate ao Câncer - SPCC:

1. Você reconhece que é maior de idade, leu, entendeu e concorda em se submeter a este termo.

2. O serviço de rede sem fio (Wi-fi) é fornecido pela SPCC e fica totalmente a seu critério seguir com o acesso.

3. O Wi-fi visitante é uma cortesia e seu acesso à rede pode ser bloqueado, suspenso ou encerrado a qualquer momento por motivos técnicos ou administrativos a qualquer momento e sem aviso prévio.

4. Não coletamos dados pessoais para sua conexão.

5. Você concorda em não usar a rede sem fio para qualquer finalidade que seja ilegal e assume total responsabilidade por seus atos.

6. Alguns sites e serviços estão bloqueados com o objetivo de garantir a integridade, segurança, zelar pelo bom uso do recurso ou por estarem em não conformidade com as políticas da SPCC.

7. Está ciente e concorda que serão coletadas informações de conexão do seu equipamento como IP, sistema operacional, mac address, data e hora da conexão, access point conectado, intensidade de sinal, quantidade de dados trafegados e os dados podem ficar armazenados por até 7 dias.

8. As informações coletadas poderão ser compartilhadas pela SPCC com: (i) demais empresas parceiras, quando forem necessárias para a adequada prestação dos serviços objeto de suas atividades; (ii) para proteção dos interesses da SPCC em qualquer tipo de conflito; (iii) mediante decisão judicial ou requisição de autoridade competente.

9. Está ciente e concorda que suas informações também poderão ser compartilhadas com empresas provedoras de infraestrutura tecnológica, operacional e de serviço de armazenamento de dados necessária para as atividades da SPCC.

10.A SPCC não se responsabiliza pelas políticas e práticas de coleta, uso e divulgação (incluindo práticas de proteção de dados) de outras organizações, incluindo todos os Dados Pessoais que divulga para outras organizações por meio dos aplicativos ou

páginas em mídias sociais, mesmo que conectado em nossa rede sem fio. Informe-se sobre a política de privacidade de cada site visitado.

11. A SPCC adota as medidas técnicas e organizacionais conforme Lei Geral de Proteção de Dados - LGPD (Lei Nº 13.709, de 14 de agosto de 2018) para preservar a privacidade dos dados coletados em suas Páginas e/ou serviços.

12.Esclarecimentos ou solicitações quanto a dados pessoais podem ser solicitadas ao DPO (Encarregado de Dados) no e-mail dpo@hcp.org.br.

13.Incidentes de segurança de dados ou informações podem ser solicitadas pelos e-mails: Unidade HCP: infra@hcp.org.br. HCP Gestão e unidades sob gestão: infra@hcpgestao.org.br

ANEXO IV:

TERMO DE CONCESSÃO DE EQUIPAMENTO DE TI

Esse Termo é referente à concessão de equipamentos de TI, de propriedade da Sociedade Pernambucana de Combate ao Câncer - SPCC. Este equipamento é uma importante ferramenta de trabalho e como tal deverá ser recebida. Este termo foi elaborado com base nos princípios gerais que norteiam o comportamento profissional e política aplicada na SPCC.

A entrega do(s) Equipamento(s) de Informática ao usuário está vinculada ao preenchimento e assinatura deste Termo de Responsabilidade. Confira todos os itens abaixo descritos.

Nome:	**Desc. Equipamento:**
ID Funcional:	**Num Série:**
Depto:	**Patrimônio:**

OBSERVAÇÕES

É vedado ao usuário utilizar o equipamento, para qualquer outra finalidade que não seja aquela ligada diretamente às atividades da sua área de atuação ou da empresa.

A instalação e a atualização de qualquer software somente serão efetuadas pelo departamento de TI. As instalações de softwares adicionais aos instalados no equipamento devem ser solicitadas diretamente ao departamento de TI via service desk (chamado).

O usuário responsável pelo equipamento não poderá em qualquer hipótese: Realizar cópias dos softwares nele instalados, instalar ou permitir a instalação de softwares por terceiros.

Esses atos são considerados ilegais e qualquer infração, danos financeiros, e outras implicações legais devido a essa prática são de inteira responsabilidade do usuário infrator – ficando sujeito às penalidades previstas na Lei Trabalhista.

O equipamento deverá ser mantido em perfeito estado de conservação e em condições normais de uso em todo período de sua utilização.

A não devolução, perda ou devolução do(s) equipamento(s) danificado (mau uso) ou faltando acessórios, será descontado em folha de pagamento o correspondente ao valor de mercado do equipamento, seus acessórios e/ou parte danificada ou faltante.

Nos casos de roubo/furto deverá ser formalizado, de imediato, queixa no órgão público competente (delegacia de polícia mais próxima) apresentando à empresa, através do service desk, o Boletim de Ocorrência (BO) correspondente para que seja providenciado as tratativas pertinentes quanto a segurança dos dados e equipamento. Neste caso, o funcionário não será responsável pela reposição do equipamento.

Declaro ter lido detidamente o texto acima e externo minha concordância às condições e termos nele constantes.

Recife, __/__/_____

_____

Assinatura

ANEXO V:

TERMO DE CONCESSÃO DE LINHA MÓVEL, SMARTPHONE

Esse Termo é referente a concessão de telefone celular e linha corporativa, de propriedade da Sociedade Pernambucana de Combate ao Câncer de Pernambuco - SPCC, destinados aos colaboradores, terceirizados e prestadores de serviço que necessitam utilizar o referido recurso para executar as suas atividades profissionais relacionadas a SPCC. Este termo foi elaborado com base nos princípios gerais que norteiam o comportamento profissional e política aplicada na empresa. A entrega dos equipamentos está vinculada ao preenchimento e assinatura deste Termo de Responsabilidade.

Confira todos os itens abaixo descritos, caso exista divergência entre a relação abaixo e o material entregue, recuse o recebimento e solicite as devidas alterações.

Nome:	**ID Funcional:**
Setor:	**Num. Linha:**
MEI CHIP:	**Modelo:**
IMEI Aparelho:	**Valor:**
Carregador:	**Fone:**
Obs:	

É vedado ao usuário utilizar o equipamento, para qualquer outra finalidade que não seja aquela ligada diretamente às atividades da sua área de atuação ou da empresa

O celular deverá ser mantido em perfeito estado de conservação e em condições normais de uso em todo período de sua utilização.

A execução/acompanhamento dos serviços de manutenção será de responsabilidade do usuário. Todas as revisões e reparos deverão ser sempre realizados em assistências técnicas autorizadas pelo fabricante.

A não devolução, perda ou devolução do aparelho danificado (mau uso) ou faltando acessórios, será descontado em folha de pagamento ou na nota fiscal de prestação do serviço o correspondente ao valor de mercado do equipamento, seus acessórios ou da parte danificada ou faltante.

Nos casos de roubo/furto deverá ser formalizado, de imediato, queixa no órgão público competente (delegacia de polícia mais próxima) apresentando à SPCC, através do suporte da TI, o Boletim de Ocorrência (BO) correspondente para que seja providenciado o bloqueio da referida linha, aparelho e iniciado o processo de substituição do equipamento.

Declaro ter lido detidamente o texto acima e externo minha concordância às condições e termos nele constantes.

Recife,_____/_____/_____ Ass:_____

ANEXO VI:

TERMO DE RESPONSABILIDADE, SIGILO E CONFIDENCIALIDADE PARA ACESSO E UTILIZAÇÃO DOS SERVIÇOS DE TI

Seja bem-vindo! Você está recebendo sua conta de acesso para os serviços de TI e declara conhecer, concordar e respeitar a Política de Segurança da Informação, Política de Privacidade, Manual de Conduta e Manual do Colaborador. O não cumprimento, de quaisquer um desses, é considerado falta grave e por isto pode acarretar sanções disciplinares, entre elas o encerramento do vínculo profissional ou contrato de serviço.

Orientações:

ACESSO À REDE CORPORATIVA:

Seu usuário e senha de acesso são pessoais e intransferíveis e seu compartilhamento é terminantemente proibido. No primeiro logon é obrigatório a alteração de senha inicial,

1. A senha deve atender aos requisitos de complexidade: mínimo 8 (oito) dígitos, caracteres especiais (!, @, #, $, %, &, *, (,), +, - , etc.);

2. A cada 60 dias será solicitada a troca da senha automaticamente. Não é permitido a utilização das últimas 3 senhas e não deixe-a à vista dos outros;

3. A cada 5 tentativas inválidas a senha será automaticamente bloqueada. Em caso de esquecimento da senha, a redefinição de senha deverá ser requisitada ao Depto. de TI.

DAS SUAS RESPONSABILIDADES COMO USUÁRIO DOS SERVIÇOS DE TI:

1. Utilizar os recursos computacionais da forma adequada, recomendada pelos fabricantes. Qualquer dano ou prejuízo causado por mau uso dos equipamentos será de sua inteira e total responsabilidade;

2. Utilizar os recursos computacionais exclusivamente para atividade profissional

3. Em cada computador há uma unidade de rede, na qual deverá salvar seus trabalhos de cunho profissional. Diariamente é realizado Backup dos arquivos contidos nesta unidade. Isentando o Departamento de TI por dados salvos em outros locais;

4. Ao ocorrer uma infração referente às Normas ou Políticas estabelecidas sua conta é desativada e será encaminhado para seu superior para análise do caso. Normas e Políticas disponíveis na intranet.

5. Você se compromete a não coletar, armazenar, processar, compartilhar ou eliminar dados pessoais ou dados pessoais sensíveis com terceiros ou setores que não tenham uma finalidade e necessidade específica à sua atribuição ou que infrinjam a Lei Geral de Proteção de Dados nº 13.709/2018.

DO USO DO MV:

1. Os ícones para acesso estão em sua área de trabalho;

2. Seu login e senha são sua identidade no Sistema, portanto é pessoal, intransferível e de sua inteira responsabilidade;

3. Todas as solicitações de acessos aos módulos, programas ou criação de novas contas de acesso, deverão ser realizadas no Service Desk conforme Política de Segurança da Informação.

DO USO DE SOFTWARE:

1. Os softwares instalados nos equipamentos atendem a Lei nº 9609/98 (Lei de Software) e Lei nº 9609/98 (Lei dos Direitos Autorais), assim, nenhum software deve ser instalado sem o devido licenciamento ou sem prévia autorização do Depto. de TI;

2. Qualquer usuário encontrado copiando software ou cedendo software da empresa a terceiros ou instalando software não regular, fica sujeito à rescisão do contrato de prestação de serviço e à rescisão de contrato de trabalho por Justa Causa, com base no artigo 482 da C.L.T., assim como à responsabilidade pessoal por tais atos;

3. Periodicamente é realizado inventário de software, a fim de constatar e verificar a existência de softwares não originais que, caso existam, implicará na remoção imediata das cópias irregulares sem aviso prévio.

DO USO DO E-MAIL CORPORATIVO E OUTRAS FERRAMENTAS:

1. Para acessar sua conta de e-mail acesse: https://webmail.hcp.org.br;

2. Não utilize o e-mail corporativo para a troca de mensagens que façam parte de correntes ou assuntos particulares;

3. Não realize cadastro em sites da Internet de assuntos pessoais com o e-mail corporativo;

4. Ao mandar e-mail com cópia para mais de uma pessoa certifique-se que todos os destinatários realmente têm relação com o assunto e necessitam ser notificados do conteúdo enviado;

5. Qualquer e-mail que você enviar pode ser compartilhado pelo destinatário para outras pessoas. Portanto, seja objetivo e profissional;

6. Tenha o mesmo cuidado, precaução e gentileza que teria com uma comunicação verbal ao enviar um e-mail. Tenha certeza que a mensagem que você enviar não seja considerada abusiva, obscena, ofensiva, profana ou preconceituosa;

7. É recomendável que as mensagens estejam com o campo “Assunto” preenchido, para facilitar a filtragem e suas prioridades;

8. A não utilização (inatividade) de sua conta por um período de tempo maior que 45 dias, a mesma será desativada sem aviso prévio.

DO USO DA INTERNET

O uso da Internet é permitido e encorajado desde que sua utilização seja aderente aos objetivos e atividades fins desempenhadas por você. O mau uso desta facilidade pode ter impacto negativo sobre a sua produtividade além do que, todos os recursos tecnológicos existem para o propósito exclusivo da SPCC.

É estritamente proibido e inaceitável:

1. Visitar sites da Internet que contenham material obsceno e/ou pornográfico.

2. Usar o computador para executar quaisquer tipos ou formas de fraudes ou software/música pirata.

3. Usar a Internet para enviar material ofensivo ou de assédio para outros usuários.

4. Baixar (download) software comercial ou qualquer outro material cujo direito pertença a terceiros (copyright), sem ter um contrato de licenciamento ou outros tipos de licenças.

5. Executar atividades que desperdicem os esforços do pessoal técnico ou dos recursos da rede.

6. Compartilhar dados pessoais e dados pessoais sensíveis que desrespeitem a Política de Privacidade.

SERVICE DESK

Service Desk corresponde a uma "central de serviços", cujo objetivo é prover aos usuários de TI um ponto único de contato entre os usuários e a equipe de TI, visando o restabelecimento da operação normal dos serviços de TI o mais rápido possível. Para abrir seu ticket de suporte (chamado) acesse: https://suporte.hcp.org.br/

Nome:		Matrícula:	
Usuário Windows		Senha Inicial:	
e-mail:		Senha Inicial:	
Usuário MV:		Senha Inicial:	

DECLARAÇÃO DE CONCORDÂNCIA COM O TERMO DE RESPONSABILIDADE, SIGILO E CONFIDENCIALIDADE PARA ACESSO E UTILIZAÇÃO DOS SERVIÇOS DE TI

Eu,_____, matrícula _____ declaro ter recebido orientações pertinentes ao uso, zelo, sigilo, confidencialidade e guardas das informações de acesso aos serviços de TI e afirmo estar de pleno acordo a zelar pela segurança e privacidade dos dados, não sendo cabível, em hipótese alguma, a alegação de não ter recebido as devidas orientações.

_____ _____

Data Assinatura do Titular do Acess

18. Atualizações

A tabela abaixo relaciona os campos necessários para o controle das atualizações, revisões e aprovações do manual de processo, a serem preenchidos sempre que julgado necessário.

33

CONTROLE DE VERSÕES E ALTERAÇÕES				
Versão	**Data**	**Responsável**	**Tipo de Alteração**	**Revisor/Aprovador**
1	14/04/2022	João Job	Criação da Política	Cleison/Mayara
2	06/05/2022	João Job	Revisão dos termos de responsabilidade.	Cleison/Mayara
3	10/06/2022	João Job	Revisão Termo de Responsabilidade, sigilo e confidencialidade	Aline Costa
4	21/06/2022	Danusa Albuquerque	Padronização	Renata Galindo

ELABORADOR	Cleison Luciano Coordenador Infra de TI Hospital do Câncer de PE Cleison Luciano	Mayara Souza HCP T.I. Mayara Souza
HOMOLOGADOR	João Job HCP T.I. João Job	Josenildo Sá Superintendente Controladoria Geral Hospital do Câncer de Pernambuco Josenildo Sá
APROVADOR	Renata Galindo Renata Galindo HCP Gerente de Qualidade	APROVADO PELA QUALIDADE
DATA DA EMISSÃO: 28/06/2022	REVISÃO: nº 04	DATA DA ÚLTIMA REVISÃO: 28/06/2022 TEMPO DE VIGÊNCIA: 24 meses