POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA UCEFF - PSI

1 INTRODUÇÃO

De forma a valorizar o trabalho institucional, de maneira idônea e responsável, estabelecem-se aqui regras, normas, diretrizes e orientações acerca das áreas competentes à tecnologia da informação e telecomunicações. Para tal, serão abordados abaixo conjuntos de instruções direcionadas ao usuário, contendo procedimentos a serem adotados visando melhores resultados e um melhor provimento das melhores técnicas de segurança. Tudo isso para uma gestão eficaz dos recursos de rede, software e hardware, bem como proteção aos ativos de informação da Instituição.

A Política de Segurança da Informação da UCEFF é o documento que apresenta e regulamenta as diretrizes corporativas da UCEFF para a proteção de todos os ativos de informação e a prevenção de responsabilidade legal para todos os usuários. O documento apresenta toda a política relacionada a segurança da informação, assim como a atualização e manutenção dos equipamentos de tecnologia da informação da Instituição para sempre manter e melhorar o funcionamento dos serviços oferecidos pela UCEFF.

Trata-se de um trabalho de equipe envolvendo a participação e colaboração de todos os colaboradores e afiliados da UCEFF que manipulam informações e/ou sistemas de informações. É de responsabilidade de cada usuário de computador conhecer esta política e conduzir suas atividades de acordo com a mesma. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

2. OBJETIVOS

O objetivo e propósito desta política de segurança da informação é assegurar e delinear a utilização aceitável e de maneira adequada dos equipamentos tecnológicos. Todos os usuários devem ter conhecimento das regras para utilização da informação de maneira segura, evitando expor qualquer informação que possa prejudicar ou lesar a UCEFF, seus colaboradores, alunos ou parceiros.

Objetiva-se com esta política preservar as informações da UCEFF quanto à:

- Integridade: Resume-se à garantia de que a informação não tenha sido alterada, e que mantenha-se em seu estado original.
- Confidencialidade: Garante que o acesso à determinados arquivos, softwares ou documentos seja destinado somente ao pessoal autorizado para tal.
- Disponibilidade: Faz com que determinada informação, arquivo, documento ou software esteja sempre disponível para os usuários que tenham autorização para acessar e que se faça necessário.

Neste sentido, esta Política de Segurança e Informação organiza e efetiva controles e normas para preservar os interesses dos colaboradores, professores, alunos e demais parceiros contra qualquer tipo de prejuízo ou infortúnio que possa vir a acontecer devido alguma falha de segurança. Ela deve descrever as normas de utilização e possíveis atividades que possam ser consideradas como violação ao uso dos serviços e portanto, considerados proibidos. Objetiva-se que com o conhecimento da Política de Segurança ocorra a utilização apropriada de todos os recursos tecnológicos da UCEFF, garantindo a segurança da própria Instituição e de todos os que se utilizam dos serviços e recursos colocados à disposição.

Todos os serviços, sistemas e equipamentos de propriedade da IES são objetos da Política de Segurança, incluindo: computadores, notebooks, contas de e-mail, dados e informações armazenadas em diretórios da rede, sistemas de aplicação e internet, bem com bem como equipamentos de propriedade de terceiros que sejam confiados a UCEFF a qualquer título, ou cedidos pela mesma a terceiros.

A política necessita ser clara e compreensível de maneira a fornecer aos interessados as informações suficientes para terem conhecimento de como os procedimentos descritos na Política de Segurança são aplicáveis a ele ou não, utilizando-se de uma linguagem simples e de fácil entendimento por todos. Ela aplica-se à todos os usuários dos sistemas, computadores ou outros recursos tecnológicos da rede da UCEFF, incluindo: colaboradores, estagiários, docentes, discentes, visitantes, prestadores de serviços temporários, colaboradores que estejam a serviço da UCEFF incluindo toda a mão-de-obra terceirizada ou disponibilizada mediante convênios, parcerias ou quaisquer outras formas de atuação conjunta com outras

empresas e demais pessoas e/ou grupos que venham a integrar, prover ou atualizar, direta ou indiretamente algum serviço da UCEFF.

As normas descritas neste documento são fornecidas para conhecimento e orientação de todos os colaboradores, alunos, terceiros e demais envolvidos, podendo as dúvidas serem esclarecidas junto ao Núcleo de Tecnologia da Informação (NTI).

Assim que necessário as normas descritas na Política da Segurança poderão sofrer alterações, sendo todas elas registradas e divulgadas pela própria UCEFF, considerando o tempo hábil para que possam ser tomadas eventuais providências.

Caso exista a violação dos termos e normas dispostos e estabelecidos neste documento, a Reitoria da UCEFF se reserva de o direito de aplicar as punições cabíveis aos usuários responsáveis pela violação da política.

3. POLÍTICA DE SEGURANÇA DA ESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO

Serão abordados neste tópico todos os itens relacionados a utilização da estrutura e rede, administração de contas, senhas, correio eletrônico, acesso a internet cabeada e sem fio, uso das estações de trabalho, utilização de impressoras ou qualquer equipamento eletrônico, entre outros.

3.1. POLÍTICA DE UTILIZAÇÃO DA REDE

Neste item serão apresentadas as normas de utilização da rede que compreende a manutenção e acesso de arquivos no servidor, acesso à rede mediante login e tentativas de acesso não autorizadas. Estes itens se aplicam à todos os usuários dos sistemas e da rede de computadores da UCEFF.

3.1.1 Regras Gerais

- Tentativas para obtenção de acesso não autorizado não serão permitidas, tais como tentativas que procuram fraudar a autenticação de usuário ou segurança de qualquer

servidor, de contas ou da rede. Isso compreende o acesso indevido a dados não disponíveis para o usuário ou de qualquer dado ao qual ele não possua direito de acesso, tentativas de conexão com o servidor ou conta cujo acesso são seja expressamente autorizado ao usuário, qualquer ação maliciosa que coloque à prova a segurança de outras redes;

- Tentativas de interferir nos serviços de qualquer outro usuário, servidor, serviço ou rede não serão permitidas. Isso inclui ataques e tentativas de provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de “invadir” um servidor;
- Não é permitido que sejam realizadas alterações das configurações da rede e das máquinas, ou outros tipos de modificações que não sejam justificadas e efetuadas pelo Núcleo de Tecnologia da Informação.
- Ao ausentar-se do seu local de trabalho ou deixar sua estação de trabalho por um longo período de tempo, é necessário que o usuário feche todos os programas em uso, precavendo e evitando desta maneira o acesso indevido por pessoas não autorizadas. É necessário que seja efetuado o logout/logoff da rede ou bloqueio do computador através de senha, que deverá ser informada ao Núcleo de Tecnologia da Informação.
- Não é permitida a instalação ou remoção de programas/softwares de qualquer natureza sem autorização e sem acompanhamento da equipe técnica do Núcleo de Tecnologia da Informação.
- O acesso à conteúdos impróprios na internet, assim como o acesso a materiais de natureza pornográfica e racista não são permitidas, bem como é vedada sua exposição, armazenamento, distribuição, edição ou gravação através de recursos tecnológicos da rede ou em equipamentos da UCEFF;
- Não poderão ser instalados, gravados ou copiados qualquer tipo de jogo que não seja para fins educacionais nos diretórios pessoais dos usuários, bem como em qualquer outro diretório da rede, ou computadores disponibilizados pela instituição.
- Não é permitido criar e/ou remover arquivos fora da área alocada ao usuário e/ou que possam comprometer o desempenho e funcionamento dos sistemas, salvo casos de arquivos que necessitam ser compartilhados com outros usuários, de um mesmo setor ou não ou que sejam de uso comum à todos os colaboradores;

- É necessário e de responsabilidade do usuário realizar a manutenção no seu diretório pessoal periodicamente, evitando o acúmulo de informações desnecessárias;
- Material de uso pessoal, de cunho sigiloso ou de natureza específica não poderão ser armazenados e/ou compartilhados na pasta pública ou similar. Este diretório deve ser utilizado apenas para armazenar informações de interesse geral;
- Periodicamente será realizada a limpeza dos arquivos armazenadas na pasta pública ou similar pela equipe do Núcleo de Tecnologia da Informação, evitando o acúmulo desnecessário de informações e degradação do acesso ao ambiente de rede;
- Quanto à utilização de equipamentos particulares, computadores, impressoras, entre outros, a UCEFF não fornecerá acessórios, software ou suporte técnico, incluindo assistência para recuperar perda de dados decorrentes de falha humana, ou pelo mau funcionamento do equipamento ou do software;
- São responsáveis sobre a licença de softwares instalados em computadores e/ou dispositivos particulares seus proprietários.
- A UCEFF não se compromete a fornecer equipamentos para consultores, professores ou terceiros, para atividades particulares ou que sejam desenvolvidas fora das suas instalações;

- O acesso aos sistemas institucionais e sistemas de gestão acadêmica, bem como de outros, deve ser controlado pela identificação do usuário e pelas senhas designadas para usuários autorizados. As senhas são de uso pessoal.

- O acesso a rede wifi da instituição está condicionado às mesmas regras de acesso à rede.

3.1.2 Regras para os colaboradores da UCEFF

- Todos os arquivos intrínsecos à Instituição devem ser armazenados no servidor de arquivos próprio para tal, a fim de protegê-los e garantir a cópia segura dos mesmos.
- Quando um empregado é transferido entre departamentos, o coordenador que transferiu deve certificar-se de que todos os direitos de acesso aos sistemas e outros controles de segurança ainda serão necessários na sua nova função e informar a equipe do NTI qualquer modificação necessária;

- Quando ocorrer o desligamento do empregado, o coordenador responsável deve informar à equipe do NTI para providenciar a desativação dos acessos do usuário à qualquer recurso a rede e sistemas aplicativos. Deve-se verificar a necessidade de troca de senhas de contas de uso comum ao departamento, evitando o acesso às informações.

- Não é permitida a abertura ou rompimento de lacres de qualquer computador ou equipamento tecnológico a fim de efetuar reparos. Caso seja necessário o reparo, este deverá ser feito pelos técnicos do Núcleo de Tecnologia.

3.1.3 Regras para estudantes e professores

- O conteúdo das contas de usuário relativos aos materiais de professor/estudante armazenados nos diretórios relativos às salas de aula, serão apagados após a sua utilização, devendo o professor responsável manter as devidas cópias caso seja necessário.

3.2. POLÍTICA DE ACESSO À INTERNET

A Internet é uma ferramenta de estudo/trabalho e deverá ser utilizada somente para este fim por quem quer que seja que venha a dela utilizar-se, não sendo permitido seu uso para fins recreativos durante o horário de trabalho ou aula.

3.2.1 Regras Gerais

- Toda a navegação e utilização da rede de internet da instituição está sujeita às sanções do Marco Civil da Internet (LEI Nº 12.965, DE 23 DE ABRIL DE 2014).
- A UCEFF conta com o direito de permitir/bloquear o acesso à sites que possam colocar em risco ou comprometer o desempenho dos ativos de segurança e dos processos dos usuários.
- São proibidos os acessos a sites com jogos, chats, apostas, material de cunho sexual ou moralmente proibido por lei.
- Caso julgue pertinente, a UCEFF se reserva ao direito de monitorar todos os acessos e origens que forem acessados em seus domínios.

- É vetada a explanação e/ou divulgação de informações que possam comprometer ou divulgar informações sensíveis à UCEFF, sendo passível de penalidades previstas nas políticas ou na forma da lei.
- É proibido acessar, copiar ou manter programas, músicas, filmes, vídeos, etc. de outras pessoas que tenham direitos autorais ou que violem a propriedade intelectual, bem como tudo que contenha em seu conteúdo material ilegal, pornográfico, discriminatório, racista ou que faça apologia ao crime.

3.2.2 Regras para Colaboradores

- Poderão ser realizados relatórios com a coleta de todos os dados e/ou websites visitados pelo usuário. Também poderá ser feita publicação do mesmo e que este tenha de prestar contas.
- É vetado o upload de qualquer natureza de arquivo ou software de propriedade ou licenciado para a UCEFF, sem a expressa autorização.
- Apenas será permitida a instalação de programas com a supervisão do responsável ou coordenador de setor em conjunto com o NTI. Também serão verificadas as licenças de uso de software antes da instalação.

3.3. POLÍTICA DE ADMINISTRAÇÃO DE CONTAS

A política de administração de contas define as normas de utilização e administração de contas que compreende a criação da mesma, manutenção e desativação.

3.3.1 Regras Gerais

- À equipe do Núcleo de TI é reservado o direito de desativar uma conta de usuário, caso seja verificado a ocorrência de algum incidente referente à suspeita de quebra de segurança nas contas dos usuários ou reincidência na quebra de senhas por programas utilizados pelo NTI.

3.3.2 Regras para Colaboradores

3.3.2.1 Solicitação de usuário/acesso

- Todo colaborador da Instituição poderá ter uma conta para acesso aos recursos da rede de computadores da UCEFF, incluindo os sistemas de gestão acadêmica, sites para uso institucional e de acesso exclusivo dos colaboradores, além de possuir um e-mail institucional. Caso seja necessário o acesso a outros sistemas o coordenador do setor deve informar ao Núcleo de TI os demais acessos necessários, sendo liberado o acesso ao usuário em questão, as permissões e a criação de conta, caso necessário.
- Quando da criação de contas para novos usuários os coordenadores e/ou responsáveis de cada setor devem solicitar por meio de e-mail ao NTI a criação da conta, informando os dados do funcionário/colaborador, bem como os acessos que serão necessários para que este usuário desempenhe suas funções na área. O NTI retornará para a coordenação do setor as informações sobre a conta criada.

3.3.2.2 Manutenção de contas

- Será destinado local específico no servidor para cada colaborador poder gravar seus arquivos pessoais, assim como os de interesse de seu setor. Diariamente será realizado backup dos arquivos dos colaboradores.
- Arquivos em contas pessoais serão de responsabilidade de cada colaborador, dos quais também sendo que o mesmo deve evitar acúmulo de arquivos desnecessários e sempre que possível verificar o que pode ser eliminado;
- As contas podem ser monitoradas pela equipe do NTI com o objetivo de verificar possíveis irregularidades no armazenamento ou manutenção dos arquivos nos diretórios pessoais.

3.3.3 Professores, Estudantes ou Estagiários

- A criação de conta para acesso a rede de computadores da UCEFF para estudantes, colaboradores ou estagiários dependerá da necessidade de utilização. Se existir esta

necessidade o procedimento adotado deverá ser o mesmo utilizado para criação de contas para funcionários.

- A criação da conta de acesso aos sistemas da UCEFF para alunos é criado quando da efetivação da matrícula.
- A criação da conta de acesso aos sistemas da UCEFF para professores é criado quando da contratação junto ao RH.

3. 4. POLÍTICA DE UTILIZAÇÃO DE EMAIL

Todos os usuários de e-mail devem tomar ciência que a Internet opera em domínio público e que não está sob o controle da equipe do NTI. As mensagens podem estar sujeitas à lentidão e conteúdos não confiáveis. Grande parte da comunicação do dia-a-dia se dá através de e-mails. É importante também lembrar que grande parte do lixo eletrônico atual chega por este meio. Os vírus atuais são enviados automaticamente (sem a necessidade direta do remetente), isso significa que um e-mail de um cliente, parceiro ou amigo pode conter vírus e deve ser manipulado com cuidado.

3.4.1 Regras Gerais

- É necessária a utilização consciente do e-mail, evitando qualquer tipo de perturbação a outras pessoas, seja através da linguagem utilizada, frequência ou tamanho das mensagens;
- O envio de e-mail deve ser efetuado somente para pessoas que desejam recebê-los. Se for solicitada a interrupção do envio, esta deve ser acatada e o envio não deverá mais acontecer;
- É proibido o envio de grande quantidade de mensagens de e-mail (spam) que, de acordo com a capacidade técnica da Rede, seja prejudicial ou gere reclamações de outros usuários. Isso inclui qualquer tipo de mala direta, como, por exemplo, publicidade, comercial ou não, anúncios e informativos, ou propaganda política;
- Não é permitido reenviar ou propagar mensagens em cadeia (correntes) de qualquer outra forma, independente da vontade do destinatário de receber tais mensagens;

- O envio de e-mails mal-intencionados é proibido, tais como mail bombing (enviar milhares de mensagens idênticas para um mesmo endereço) ou sobrecarregar um usuário, site ou servidor com e-mail muito extenso ou com anexos muito grandes;
- Caso a UCEFF julgue necessário, haverá bloqueios:
  - ✓ De e-mail com arquivos anexos que comprometa o uso de banda ou perturbe o andamento dos trabalhos;
  - ✓ De e-mail para destinatários ou domínios que comprometam o uso de banda ou perturbem o bom andamento dos trabalhos;
  - ✓ De e-mail com utilização da linguagem indevida em respostas aos e-mails comerciais, como abreviações de palavras, uso de gírias etc;
- Torna-se obrigatória a manutenção da caixa de entrada, evitando acúmulo de e-mails e arquivos inúteis;
- Não abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos;
- Não abrir arquivos anexados com as extensões .bat, .exe, .src, .lnk e .com;
- Não abrir e-mail com assuntos estranhos e/ou em outros idiomas.
- Evitar anexos muito grandes;

3.4.2 Regras para os Colaboradores

- Não é permitido o envio de mensagens de correio eletrônico cujo conteúdo seja confidencial ou restrito à UCEFF, não podendo tornar-se público;
- Fica proibido o uso de e-mails institucionais da UCEFF ou do setor/departamento em que trabalha para fins pessoais e fora do expediente de trabalho;
- Os colaboradores poderão ter conta corporativa de correio eletrônico com a extensão do domínio da UCEFF, para uso pessoal, sendo a mesma desativada quando do desligamento do colaborador.

3.5. POLÍTICA DE SENHAS

Para acesso aos sistemas da UCEFF será necessário autenticação com usuário e senha, como forma de segurança. As senhas são utilizadas por todos os sistemas da UCEFF e são consideradas necessárias como um dos meio de autenticação. A eficácia das senhas dependem

do usuário, pois estes podem escolher senhas óbvias e fáceis de serem descobertas, ou ainda compartilhá-las com outros colaboradores, não mantendo o sigilo necessário e colocando em risco os ativos de segurança da instituição.

3.5.1 Regras Gerais

- A concessão de senhas é controlada, considerando:
  - ✓ A senha deve ser redefinida pelo menos a cada dois meses, para usuários comuns e a cada mês para usuários de acesso mais restrito;
  - ✓ As senhas devem ser bloqueadas após 3 a 5 tentativas sem sucesso, sendo que, o administrador da rede e o usuário devem ser notificados sobre estas tentativas.
  - ✓ Senhas temporárias devem ser alteradas imediatamente, não devem ser armazenadas de forma desprotegida,
- Aos administradores dos sistema fica a responsabilidade quanto ao cuidado na criação e alteração das senhas dos usuários, além da necessidade de manter atualizados os dados dos mesmos.
- Os usuários são responsáveis por: cuidados com a manutenção da segurança dos recursos, tais como sigilo da senha e o monitoramento de sua conta, evitando sua utilização indevida. As senhas são sigilosas, individuais e intransferíveis, não devendo ser divulgadas em nenhuma hipótese.
- Os acessos que forem executados com a senha de usuário da rede ou de outro sistema serão de inteira responsabilidade do usuário. As senhas são efetivas apenas quando usadas corretamente e sua escolha e uso requerem alguns cuidados, como por exemplo:
  - ✓ Não utilizar senhas somente com dígitos ou com letras;
  - ✓ Utilizar senha com pelo menos, oito caracteres;
  - ✓ Não utilizar senhas com repetição do mesmo dígito ou da mesma letra;
  - ✓ Não fornecer senha para ninguém, por razão alguma;
  - ✓ Utilizar senhas que podem ser digitadas rapidamente, sem a necessidade de olhar para o teclado.
  - ✓ Misturar caracteres maiúsculos e minúsculos;
  - ✓ Misturar números, letras e caracteres especiais;

- ✓ Incluir pelo menos, um caractere especial;
- ✓ Utilizar um método próprio para lembrar da senha, de modo que ela não precise ser escrita em nenhum local, em hipótese alguma;
- ✓ Não utilizar palavras que estão no dicionário (nacionais ou estrangeiras);
- ✓ Não utilizar informações pessoais fáceis de serem obtidas, como o número de telefone, nome da rua, nome do bairro, cidade, data de nascimento, etc;
- ✓ Não anotar a senha em papel ou em outros meios de registro de fácil acesso;
- ✓ Não utilizar o nome do usuário;
- ✓ Não utilizar o primeiro nome, o nome do meio ou o sobrenome;
- ✓ Não utilizar nomes de pessoas próximas, como da esposa(o), dos filhos, de amigos;

3.6. POLÍTICA DE USO DAS ESTAÇÕES DE TRABALHO

Todas as estações de propriedade da UCEFF possuem numerações internas que possibilitam sua identificação única dentro da rede. Portanto, fica de responsabilidade do usuário tudo aquilo que seja executado na máquina. Desta forma, sempre que sair, este deverá se certificar de ter efetuado logoff/logout com segurança ou bloquear a estação. Entende-se por estação de trabalho qualquer computador e/ou dispositivo portátil de propriedade da UCEFF.

3.6.1 Regras Gerais

- Fica vetado gravar nas máquinas arquivos MP3, filmes, fotos e softwares não licenciados ou que não possuam licença *free*, assim como qualquer outro material que possa ser considerado pirataria;
- Todos os dados relativos à UCEFF devem ser mantidos no servidor, onde existe sistema de backup diário e confiável;
- Fica firmada responsabilidade do usuário todo e qualquer recurso digital e/ou de tecnologia disponibilizado para suas atividades na UCEFF.
- Não utilizar nenhum tipo de software/hardware sem autorização do NTI;
- É impossível a garantia de integridade, confidencialidade e disponibilidade de arquivos salvos em diretórios temporários, uma vez que as estações de trabalho podem

ser acessadas por outros usuários. Estas poderão ser alteradas ou excluídos sem aviso prévio por qualquer outro usuário que acessar aquela estação.

- Fica vetado o uso de quaisquer recursos digitais ou outros de propriedade da UCEFF para constranger, assediar, reprimir, amedrontar, prejudicar ou ameaçar a Instituição ou terceiros, sejam indivíduos ou organizações.

3.7. POLÍTICA DE SEGURANÇA FÍSICA

Sobre a abordagem da segurança física dos equipamentos de informática e das informações sensíveis da instituição.

3.7.1 Política de controle de acesso

Quanto ao controle de acesso aos colaboradores da instituição, existem áreas que requerem maior atenção, como salas com informações confidenciais e/ou equipamentos que devem ter sua segurança garantida, como a sala de servidores.

Concorda-se que o acesso à estas áreas sejam controlados de forma zelosa, para garantir que apenas pessoal autorizado tenha acesso. As instalações utilizadas para fins especiais que abrigam equipamentos importantes exigem maior proteção que o normal.

3.7.1.1 Regras Gerais

- É proibido aos usuários da rede a adição e/ou remoção de qualquer recurso tecnológico, seja microcomputadores, impressoras ou outros equipamentos e dispositivos. É necessário, em caso de adição ou remoção destes, a solicitação ao NTI, que ficará responsável por esta ação.

- Somente pessoal autorizado poderá acessar os ambientes de infraestrutura de TI da UCEFF, utilizando crachá de identificação.

- A temperatura, umidade e ventilação do ambiente dos equipamentos de tecnologia deve estar de acordo com as normas técnicas especificadas pelo fabricante.

3.7.2 Política de mesa limpa e tela limpa

A política de mesa limpa se denomina pela garantia de que informações físicas que por ventura venham a ser sensíveis não sejam expostas à terceiros sem autorização, como anotações, mídias removíveis, papéis, documentos, etc.

A política de tela limpa se denomina pela garantia de que as informações virtuais utilizadas pelos colaboradores da UCEFF não sejam expostas à terceiros, através da ociosidade do monitor que não esteja em uso no momento.

3.7.2.1 Regras Gerais

- Papéis, mídias de computador, bilhetes, anotações, etc. não devem ser mantidos sobre as mesas quando estas não estiverem sendo usadas. Deve-se guardar em gavetas ou armários trancados.
- Quando em desuso, nenhum computador pode permanecer com seus arquivos abertos/visíveis, para que as informações ali contidas não sejam visualizadas.
- Anotações, agendas, livros ou qualquer outro material que possa conter informações sobre a instituição ou informações privadas devem ser mantidas em locais fechado, sem que outras pessoas tenham acesso às informações contidas.
- Todas as chaves de armários, gavetas, portas e laboratórios devem ser mantidas em local adequado, não deixados sobre as mesas e guardados de forma negligente ou com colaboradores ou pessoas não autorizados.

3.7.3 Política de utilização de laboratórios de informática, salas de aula e auditórios

É necessário que as normas estabelecidas nesta política de segurança quanto a utilização de laboratórios e equipamentos de informática sejam cumpridas, assim como o uso correto das instalações, evitando qualquer tipo de dano aos equipamentos dos laboratórios, das salas de aula, auditórios e outros ambientes da IES.

3.7.3.1 Regras Gerais

- O acesso aos laboratórios de informática deve ser rigidamente controlado, somente sendo permitido o seu uso por usuários autorizados. É de responsabilidade do professor/funcionário que utilizou o laboratório zelar pela ordem das instalações. Caso seja necessária qualquer tipo de manutenção a equipe técnica responsável deve ser informada.

- O responsável pelo laboratório deve verificar, no momento da entrada, se todos os equipamentos estão funcionando corretamente. Após a utilização, esta verificação deve ser repetida e qualquer problema deve ser relatado à equipe técnica do NTI para que este seja solucionado o mais rápido possível.
- Os laboratórios devem permanecer trancados quando deixados sem supervisão.
- No momento da aula, a supervisão do laboratório é de responsabilidade do professor;
- Nenhum equipamento ou mídia pode ser conectado aos sistemas ou rede sem aprovação prévia.
- Alimentos, bebidas, fumo, etc. são proibidos nas dependências dos laboratórios, salas de servidores, auditórios etc.

4. TERMO DE COMPROMISSO

Utilizado por alunos, professores, colaboradores, estagiários, entre outros, o termo de compromisso visa comprometer os usuários em seguir as normas estabelecidas nesta Política de Segurança, estando cientes das punições em casos de negligência, erros e/ou outros motivos abaixo esclarecidos. Neste termo são destacados os principais pontos desta política de segurança, devendo ser assinado por todos os funcionários/colaboradores ligados à instituição. Deve-se efetuar sua renovação sempre que necessário.

5. AUDITORIA

Para garantir que as normas mencionadas acima estão sendo cumpridas, a UCEFF se reserva no direito de:

- Instalar sistemas que monitorem o consumo e o uso da Internet dentro da instituição, através de armazenamentos internos e diretamente dentro das máquinas.
- Verificar os arquivos armazenados na rede, seja em áreas privadas ou nos discos rígidos das máquinas analisadas.
- Realizar vistorias periódicas em computadores/notebooks aleatórios a fim de verificar inconsistências e/ou relatar riscos. Em caso de comprovada inconformidade com as políticas de segurança, serão levados em consideração a gravidade da violação das normas e tomadas as medidas cabíveis.

6. VIOLAÇÃO DA POLÍTICA, ADVERTÊNCIA E PUNIÇÕES

- No momento em que uma violação é detectada, o primeiro passo é determinar o motivo: verificar se a mesma ocorreu por negligência, erro, acidente ou desconhecimento da política.
- Caso seja detectado uso incoerente com o intuito de violar o andamento do trabalho, ou prejudicar algum sistema e/ou indivíduo, a UCEFF bloqueará o acesso ou poderá efetuar o cancelamento do usuário, a fim de evitar riscos à imagem da instituição.
- É de fundamental importância e recomenda-se o treinamento dos usuários em conceitos básicos de segurança da informação, uma vez que sua divulgação e conscientização é de suma importância e deverá ser seguida por todos. É real a necessidade de um programa de treinamento em segurança da informação ao início de cada ano letivo (novos alunos) e na integração de novos colaboradores à equipe UCEFF. Treinamentos de reciclagem também são importantes e devem ser previstos quando a Instituição julgar necessário.

6.1 Regras para Colaboradores

- Em caso de necessidade de advertência ao funcionário, a situação será informada imediatamente ao Departamento de Recursos Humanos.
- Caso seja comprovado o descumprimento pelo funcionário das normas estabelecidas, em fatos isolados ou geral, poderá acarretar, com base no delito, punições como: Comunicação de descumprimento, Advertência, Suspensão ou demissão por justa causa.

6.2 Regras para alunos

- Em caso de necessidade de advertência ao aluno, a situação será informada imediatamente à Secretaria Acadêmica.
- Caso seja comprovado o descumprimento pelo aluno das normas estabelecidas, em fatos isolados ou geral, poderá acarretar, com base no delito, punições como: Comunicação de descumprimento, Advertência, Suspensão ou Expulsão.

7. DISPOSIÇÕES FINAIS

Os casos omissos serão dirimidos pela coordenação do NTI, bem como pela administração da UCEFF.

ANEXO I – TERMO DE COMPROMISSO

TERMO DE COMPROMISSO

Identificação do Funcionário/Colaborador

COD.	EMPREGADOS	CPF	SETOR	ASSINATURA

Comprometo-me a:

1. Executar minhas tarefas de forma a cumprir com as orientações da Política de Segurança da UCEFF e com as Normas e Padrões vigentes.
2. Utilizar adequadamente os equipamentos da Instituição, evitando acessos indevidos aos ambientes computacionais aos quais estarei habilitado, que possam comprometer a segurança das informações.
3. Não revelar fora do âmbito profissional, fato ou informações de qualquer natureza que tenha conhecimento devido a minhas atribuições, salvo em decorrência de decisão competente do superior hierárquico.
4. Acessar as informações somente por necessidade de serviço e por determinação expressa do superior hierárquico.
5. Manter cautela quando a exibição de informações sigilosas e confidenciais, em tela, impressoras ou outros meios eletrônicos.
6. Não me ausentar do local de trabalho sem encerrar a sessão de uso do computador ou sistema, evitando assim o acesso por pessoas não autorizadas.
7. Observar rigorosamente os procedimentos de segurança estabelecidos quanto à confidencialidade de minha senha, através dos quais posso efetuar operações a mim designadas nos recursos computacionais que acesso, procedendo a:
    a. Substituir a senha inicial gerada pelo sistema, por outra secreta, pessoal e intransferível;
    b. Não divulgar a minha senha a outras pessoas;
    c. Nunca escrever a minha senha, sempre memorizá-la;

d. De maneira alguma ou sobre qualquer pretexto, procurar descobrir as senhas de outras pessoas;
e. Somente utilizar o meu acesso para os fins designados e para os quais estiver devidamente autorizado, em razão de minhas funções;
f. Responder em todas as instâncias, pelas conseqüências das ações ou omissões de minha parte que possam por em risco ou comprometer a exclusividade de conhecimento da minha senha ou das transações a que tenho acesso;
g. Reportar imediatamente ao superior imediato ou ao Administrador de Segurança em caso de violação, acidental ou não, da minha senha, e providenciar a sua substituição.
h. Solicitar o cancelamento de meus usuário/senhas quando não for mais de minha utilização.
i. Solicitar o cancelamento de usuários/senhas solicitados para funcionários/terceiros sob minha responsabilidade, quando do seu desligamento ou término do serviço que originou a respectiva solicitação.

Declaro estar ciente das determinações acima, compreendendo que quaisquer descumprimentos dessas regras podem implicar na aplicação das sanções disciplinares cabíveis.

Itapiranga - SC, _____ de _____ de _____.

_____

Responsável pelo Núcleo de Tecnologia da Informação