POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA UCEFF - PSI

1 INTRODUÇÃO

Procurando agregar valor ao trabalho da IES, através do melhor uso dos recursos disponíveis e para que se obtenham melhores resultados, faz-se necessário estabelecer normas e diretrizes que englobam todas as áreas relacionadas à tecnologia da informação, inclusive telecomunicações. Portanto, neste documento será apresentado um conjunto de instruções e procedimentos para normatizar e melhorar a atuação em relação à segurança das informações e utilização dos ativos da Instituição, assim como de qualquer equipamento e software que seja relacionado à TI ou telecomunicações.

A Política de Segurança da Informação da UCEFF é o documento que orienta e estabelece as diretrizes corporativas da UCEFF para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

2. OBJETIVOS

O objetivo é garantir que os recursos de informática e a informação serão utilizados de maneira adequada. O usuário deve conhecer as regras para utilização da informação de maneira segura, evitando expor qualquer informação que possa prejudicar a UCEFF, seus funcionários, alunos ou parceiros.

A política deve ser clara o bastante para fornecer aos interessados informações suficientes para saber se os procedimentos descritos são aplicáveis a ele ou não, utilizando linguagem simples e de fácil entendimento por todos.

A Política deve implementar controles para preservar os interesses dos funcionários, professores, alunos e demais parceiros contra danos que possam acontecer devido a 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.

São objetos da Política de Segurança, os serviços e recursos colocados à disposição dos funcionários, alunos e parceiros, tais como: computadores, correio eletrônico, Internet, informações armazenadas em diretórios da rede e sistemas de aplicação.

As normas descritas no decorrer devem sofrer alterações sempre que necessário, sendo que estas devem ser registradas e divulgadas, considerando-se o tempo hábil para que eventuais providências sejam tomadas.

Tais normas são fornecidas, a título de orientação aos funcionários, alunos e demais envolvidos. Em caso de dúvida o usuário deverá procurar o NTI visando esclarecimentos.

Caso os procedimentos ou normas aqui estabelecidos sejam violados, a direção da UCEFF se reserva o direito de aplicar as punições cabíveis aos usuários responsáveis pela violação da política.

Esta política aplica-se a todos os usuários dos sistemas ou computadores da rede da UCEFF, sendo eles: funcionários, estagiários, alunos, professores, terceiros ou visitantes.

O principal objetivo dessa política é preservar as informações da UCEFF 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.

3. POLÍTICA DE SEGURANÇA DA ESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO

A Política de Segurança da estrutura de tecnologia da informação abrange itens relacionados a utilização desta estrutura, como política de utilização da rede, administração de contas, senhas, correio eletrônico, acesso a Internet, uso das estações de trabalho, acesso a wifi, utilização de impressoras etc.

3.1. POLÍTICA DE UTILIZAÇÃO DA REDE

Esse tópico visa definir as normas de utilização da rede que abrange o LOGIN, a manutenção de arquivos no servidor e as tentativas não autorizadas de acesso. Estes itens serão abordados para todos os usuários dos sistemas e da rede de computadores da UCEFF.

3.1.1 Regras Gerais

- Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta. Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se a servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes;
- Não são permitidas tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques e tentativas de provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de "invadir" um servidor;
- Antes de ausentar-se do seu local de trabalho, o usuário deverá fechar todos os programas em uso, evitando, desta maneira, o acesso por pessoas não autorizadas, e se possível efetuar o logout/logoff da rede ou bloqueio do computador através de senha;
- O usuário deve fazer manutenção no seu diretório pessoal periodicamente, evitando o acúmulo de informações desnecessárias;
- Materiais de natureza pornográfica e racista não podem ser expostos, armazenados, distribuídos, editados ou gravados através do uso dos recursos computacionais da rede;
- Jogos ou qualquer tipo de software/aplicativo não podem ser gravados ou instalados no diretório pessoal do usuário, no computador local ou em qualquer outro diretório da rede;
- 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. Em alguns casos pode haver mais de um compartilhamento referente aos arquivos de usuários de um mesmo departamento;
- A pasta PÚBLICA ou similar, não deverá ser utilizada para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza específica. Ela deve ser utilizada apenas para armazenar informações de interesse geral;
- Será feita semestralmente a limpeza dos arquivos armazenados na pasta PÚBLICA ou similar, para que não haja acúmulo desnecessário de informações e degradação do acesso ao ambiente de rede;
- É proibida a instalação ou remoção de softwares que não sejam devidamente acompanhadas pela equipe técnica do NTI, autorizada formalmente pelo coordenador responsável pela área do solicitante;
- Não são permitidas alterações das configurações de rede e/ou das máquinas, bem como demais modificações que não sejam justificadas e efetuadas pelo NTI;
- 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;

- A UCEFF não se compromete a fornecer equipamentos para consultores, professores ou terceiros, para atividades particulares ou que sejam desenvolvidas fora das suas instalações;
- Os acessos a sistemas, como sistema acadêmico, 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 a rede.
- A responsabilidade sobre a licenças de softwares instalados em computadores e/ou dispositivos particulares é de responsabilidade de seus proprietários.

3.1.2 Regras para empregados e demais colaboradores

- É obrigatório armazenar os arquivos inerentes à instituição no servidor de arquivos para garantir a cópia de segurança dos mesmos;
- É proibida a abertura de computadores para qualquer tipo de reparo, seja em departamentos ou laboratórios. Caso seja necessário o reparo, este deverá ser feito pelo departamento técnico do NTI;
- 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.

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 ADMINISTRAÇÃO DE CONTAS

Este tópico visa definir as normas de administração das contas que abrange: criação, manutenção e desativação da conta. Esta política será dividida por usuários para facilitar o entendimento de todos.

3.2.1 Regras Gerais

- É reservado o direito de desativar uma conta de usuário, por parte da equipe de segurança do NTI, caso verifique-se a ocorrência de algum dos fatos abaixo especificados:
    - Incidentes suspeitos de quebra de segurança nas contas dos usuários;
    - Reincidência na quebra de senhas por programas utilizados pela equipe de segurança;

3.2.2 Regras para Empregados

3.2.2.1 Solicitação de usuário/acesso

- Todo empregado poderá ter uma conta para acesso aos recursos da rede de computadores da UCEFF. Os acessos a demais sistemas devem ser informados pelo coordenador da área no momento da solicitação da conta do usuário e as permissões liberadas. Para solicitação de criação de conta para novos usuários, os coordenadores devem proceder conforme descrito abaixo:
    - O coordenador de departamento a que o funcionário pertence deverá fazer uma solicitação da criação da conta, através de email ao NTI. Neste e-mail, deverá ser informado os dados do funcionário/colaborador, bem como os acessos que serão necessários para que este usuário desempenhe suas funções na área (diretórios da rede UCEFF, acesso ao sistemas, acesso ao email e Internet).
    - A equipe de segurança retornará para a coordenação do departamento as informações sobre a conta criada.

3.2.2.2 Manutenção de contas

- Cada empregado que tiver sua conta criada terá um espaço no servidor para gravar seus arquivos pessoais, e será realizada cópia de segurança dos arquivos do servidor do domínio da UCEFF diariamente;
- A manutenção dos arquivos na conta pessoal é de responsabilidade do usuário, 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 de segurança com o objetivo de verificar possíveis irregularidades no armazenamento ou manutenção dos arquivos nos diretórios pessoais.

3.2.3 Professores, Estudantes , Colaboradores 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.

3.3. POLÍTICA DE SENHAS

As senhas são utilizadas por todos os sistemas e são consideradas necessárias como meio de autenticação. A eficiência 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.

3.3.1 Regras Gerais

- Senhas são um meio comum de validação da identidade do usuário para obtenção de acesso a um sistema de informação ou serviço. A concessão de senhas deve ser controlada, considerando:
    - Senhas temporárias devem ser alteradas imediatamente, não devem ser armazenadas de forma desprotegida,
    - 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.
- As responsabilidades do administrador do sistema incluem o cuidado na criação e alteração das senhas dos usuários, além da necessidade de manter atualizados os dados dos mesmos.
- As responsabilidades do usuário incluem, principalmente, os 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.

- Tudo que for executado com a senha de usuário da rede ou de outro sistema será de inteira responsabilidade do usuário. As senhas são efetivas apenas quando usadas corretamente e sua escolha e uso requerem alguns cuidados como:
    - 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 utilizar senhas somente com dígitos ou com letras;
    - Utilizar senha com pelo menos, oito caracteres;
    - 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 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;
    - 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.

3. 4. POLÍTICA DE UTILIZAÇÃO DE e-Mail

Esse tópico visa definir as normas de utilização de e-mail que engloba desde o envio, recebimento e gerenciamento de contas.

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 técnica do NTI. As mensagens podem estar sujeitas a demora e serviços potencialmente não confiáveis.

Grande parte da comunicação do dia-a-dia passa através de e-mails. Mas é importante também lembrar que grande parte das pragas eletrônicas atuais chega por esse meio. Os vírus atuais são enviados automaticamente, isso significa que um e-mail de um cliente, parceiro ou amigo pode conter vírus.

3.4.1 Regras Gerais

- O email deve ser utilizado de forma consciente, evitando qualquer tipo de perturbação a outras pessoas, seja através da linguagem utilizada, freqüência 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;
- É proibido reenviar ou de qualquer forma propagar mensagens em cadeia, independente da vontade do destinatário de receber tais mensagens;
- É proibido o envio de e-mail mal-intencionado, tais como mail bombing (enviar vários milhares de mensagens idênticas para uma caixa de correio eletrônico) ou sobrecarregar um usuário, site ou servidor com e-mail muito extenso ou numeroso anexos ou 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;
- É obrigatória a manutenção da caixa de e-mail, evitando acúmulo de e-mails e arquivos inúteis;
- Não executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos;
- Não abrir arquivos anexados com as extensões .bat, .exe, .src, .lnk e .com se não tiver certeza absoluta que solicitou este email;
- Desconfiar de todos email com assuntos estranhos e/ou em outros idiomas.
- Evitar anexos muito grandes;

3.4.2 Regras para empregados

- Não devem ser enviadas mensagens de correio eletrônico cujo conteúdo seja confidencial ou restrito a UCEFF, não podendo tornar-se público;

- Não utilizar o email da UCEFF do setor/departamento para fins pessoais e fora do expediente de trabalho;
- Funcionários 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 ACESSO À INTERNET

Esse tópico visa definir as normas de utilização da Internet que abrange a navegação em sites, downloads e uploads de arquivos.

A Internet é uma ferramenta de trabalho e/ou estudo e deve ser usada para este fim pelos funcionários, professores e alunos da UCEFF, não sendo permitido o seu uso para fins recreativos durante o horário de trabalho ou de aula.

3.5.1 Regras Gerais

- Toda a navegação e utilização da rede de internet da instituição esta sujeita as sanções do Marco Civil da Internet (LEI Nº 12.965, DE 23 DE ABRIL DE 2014.)
- É proibida a divulgação de informações confidenciais da UCEFF em hipótese alguma, seja em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei;
- A UCEFF se reserva o direito de bloquear o acesso a arquivos e sites que exponham a rede a riscos de segurança, bem como comprometem o desempenho e a produtividade das atividades dos usuários;
- O acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas e/ou conteúdo proíbido por lei ou moralmente não serão permitidos;
- Caso julgar necessário a UCEFF poderá monitorar os acessos e conteúdo com origem em sua rede;
- Não é permitido acessar, copiar ou armazenar programas de computador ou qualquer outro material (música, fotos e vídeos) que violem a lei de direitos autorais (copyright) e ou propriedade intelectual, bem como aqueles de conteúdo ilegal, pornográfico, discriminatório, racista ou que faça apologia ao crime;

3.5.2 Regras para empregados

- A instalação de qualquer programa somente pode ser efetuado com autorização do chefes de departamento juntamente como o departamento do NTI. E também se faz necessário a regularização das licenças antes da instalação.

- Funcionários com acesso à Internet não podem efetuar *uploads* de qualquer software licenciado para a UCEFF ou de dados de propriedade da UCEFF ou de seus clientes, sem expressa autorização do responsável pelo software ou pelos dados;
- Haverá geração de relatórios dos sites acessados por usuário, se necessário a publicação desse relatório e prestação de contas do usuário dos acessos;

3.6. POLÍTICA DE USO DAS ESTAÇÕES DE TRABALHO

Cada estação de trabalho possui códigos internos os quais permitem que ela seja identificada na rede. Sendo assim, tudo que for executado na estação de trabalho será de responsabilidade do usuário. Por isso, sempre que sair de frente da estação de trabalho, o usuário deverá ter certeza que efetuou o logoff ou bloqueou a estação de trabalho. Considera-se estação de trabalho qualquer computador ou dispositivo de propriedade da UCEFF utilizado em sua rede.

3.6.1 Regras Gerais

- Não utilizar nenhum tipo de software/hardware sem autorização do NTI;
- Não é permitido gravar nas estações de trabalho MP3, filmes, fotos e software com direitos autorais ou 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;
- É de responsabilidade do usuário todo e qualquer recurso de tecnologia da informação e de telecomunicação disponibilizado para o desempenho de suas atividades profissionais e/ou acadêmicas;
- Os arquivos gravados em diretórios temporários das estações de trabalho podem ser acessados por todos os usuários que utilizarem a mesma, portanto não pode-se garantir sua integridade e disponibilidade. Poderão ser alterados ou excluído sem prévio aviso e por qualquer usuário que acessar a estação.
- Não é permitido utilizar os recursos computacionais ou quaisquer outros de propriedade da UCEFF, colocados à disposição dos usuários em razão do exercício de sua função, para constranger, assediar, prejudicar ou ameaçar a IES ou terceiros, sejam eles indivíduos ou organizações;

3.7. POLÍTICA DE SEGURANÇA FÍSICA

Neste item será abordada a segurança física dos equipamentos de informática e das informações manipuladas pela instituição.

3.7.1 Política de controle de acesso

Existem áreas que merecem maior atenção quanto ao controle de entrada de pessoas, como departamentos que manipulam informações confidenciais ou equipamentos que devem ter sua segurança física assegurada, como a sala de servidores.

Convém que o acesso a estas áreas sejam controlados de forma apropriada para assegurar que somente as pessoas previamente autorizadas tenham acesso liberado. As instalações utilizadas para fins especiais que abrigam equipamentos importantes exigem maior proteção que o nível normalmente oferecido. As instalações de TI devem ser localizadas e construídas buscando minimizar o acesso público direto, os riscos ao fornecimento de energia e aos serviços de telecomunicações.

3.7.1.1 Regras Gerais

- É vetada aos usuários da rede de computadores da organização a adição e remoção de quaisquer recursos, sejam elas microcomputadores, impressoras ou outros equipamentos e dispositivos. A adição e remoção desses deverão ser solicitadas ao setor responsável, para aprovação e, em caso positivo, tais procedimentos deverão ser realizados pelo mesmo.

- Apenas pessoas autorizadas devem acessar as instalações de infraestrutura de TI, sendo que todos os funcionários/colaboradores devem usar crachás de identificação.
- A temperatura umidade e ventilação das instalações que abrigam equipamentos de informática e de comunicações, devem estar de acordo com os padrões técnicos especificados pelos fabricantes dos equipamentos.

3.7.2 Política de mesa limpa e tela limpa

A política de mesa limpa deve ser considerada para todos os departamentos e seguida por todos os funcionários/colaboradores, de forma a garantir que papéis e mídias removíveis não fiquem expostas ao acesso não autorizado.

A política de tela limpa deve ser considerada para todos os departamentos e seguida por todos os funcionários/colaboradores, de forma a garantir que as informações manipuladas por sistemas aplicativos, planilhas, documentos etc., não fiquem expostas, permitindo o seu acesso a pessoas não autorizadas.

3.7.2.1 Regras Gerais

- Os papéis ou mídias de computador não devem ser deixados sobre as mesas, quando não estiverem sendo usados. Devem ser guardados de maneira adequada, de preferência em gavetas ou armários trancados;
- Sempre que o computador não estiver em uso, não deve-se deixar nenhum arquivo aberto, de modo que as informações possam ser visualizadas por outras pessoas que estiverem no local;
- Agendas, livros ou qualquer outro material que possa conter informações sobre a empresa ou informações particulares devem sempre ser guardadas em locais fechados, evitando o acesso de outras pessoas que não as responsáveis pela informação.
- Chaves de gavetas, armários, de portas de acesso às salas e laboratórios de informática devem ser guardadas em lugar adequado, e não deixadas sobre a mesa ou guardadas com funcionários/colaboradores não autorizados.

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

Para utilização de laboratórios e equipamentos de informática, algumas regras básicas devem ser cumpridas para que seja feito o uso correto das instalações, evitando qualquer tipo de dano aos equipamentos em laboratório, prejudicando sua utilização.

3.7.3.1 Regras Gerais

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

4. TERMO DE COMPROMISSO

O termo de compromisso é utilizado para que funcionários, alunos, professores, colaboradores e estagiários se comprometam formalmente em seguir a política de segurança, tomando ciência das punições impostas ao seu não cumprimento.

No termo de compromisso são reforçados os principais pontos da política de segurança e, deve ser assinado por todos os funcionários e colaboradores da instituição. Sua renovação deve ser feita sempre que necessário.

5. AUDITORIA

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

- Implantar softwares e sistemas que monitorem e gravem todos os usos de Internet através da rede e das estações de trabalho da empresa;
- Inspecionar qualquer arquivo armazenado na rede, estejam eles no disco local da estação ou nas áreas privadas da rede;
- A UCEFF poderá periodicamente fazer uma vistoria em computadores ou notebooks escolhidos aleatoriamente e, caso verificado alguma inconformidade, serão levantados os aspectos da gravidade da violação das normas de utilização dos equipamentos;

6. VIOLAÇÃO DA POLÍTICA, ADVERTÊNCIA E PUNIÇÕES

- Ao detectar uma violação da política, a primeira coisa a fazer é determinar a sua razão, ou seja, verificar se a violação ocorreu por negligência, acidente, erro ou por desconhecimento da política vigente.
- Nos termos da Política de Segurança, a UCEFF procederá ao bloqueio do acesso ou ao cancelamento do usuário, caso seja detectado uso indevido com o intuito de prejudicar o andamento do trabalho ou de por em risco a imagem da instituição.
- É recomendado o treinamento dos usuários em segurança da informação, com o intuito de divulgar e conscientizar os funcionários e colaboradores sobre a política de segurança a ser seguida por todos. O programa de treinamento em segurança deve fazer parte do programa de integração de novos funcionário/colaboradores e do programa de integração de novos alunos (ao início de cada ano letivo). Os treinamentos de reciclagem devem ser previstos quando necessários.

6.1 Regras para funcionários

- Caso seja necessário advertir o funcionário, deve ser informado o Departamento de Recursos Humanos para interagir e manter-se informado da situação.
- O não cumprimento, pelo funcionário, das normas estabelecidas neste documento seja isolada ou cumulativamente, poderá causar, de acordo com a infração cometida, as

seguintes punições: Comunicação de descumprimento, Advertência, suspensão ou demissão por justa causa.

6.2 Regras para alunos

- Caso seja necessário advertir o aluno, a Secretária Acadêmica será informada da situação.
- O não cumprimento pelo aluno das normas estabelecidas neste documento seja isolada ou cumulativamente, poderá causar, de acordo com a infração cometida, as seguintes punições: 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/Estudante

Nome:
RG/CPF:
Matrícula:
Empresa*:

*Nome e CNPJ, somente para terceiros

Comprometo-me a:

1. Executar minhas tarefas de forma a cumprir com as orientações da Política de Segurança 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.

Chapecó - SC, _____ de _____ de _____.

_____ _____

Gerência de Tecnologia da Informação Funcionário/Colaborador/Estudante