PORTARIA Nº 93 DE 26 DE DEZEMBRO DE 2006.

Promove a implantação de Normas e Política de Segurança no âmbito do CFMV e dá outras providências.

O PRESIDENTE DO CONSELHO FEDERAL DE MEDICINA VETERINÁRIA - CFMV, no uso das atribuições que lhe são conferidas pelo art. 17, da Lei nº 5.517/68, combinado com as alíneas "b" e "l" do art. 4º do Regimento Interno do CFMV aprovado pela Resolução nº 04, de 28 de julho de 1969, e

considerando a necessidade de regulamentar a utilização dos serviços de tecnologia da informação no âmbito da estrutura organizacional do CFMV para melhor atender as necessidades finalísticas da Instituição.

R E S O L V E:

Art. 1º Implantar Normas e Política de Segurança para regulamentar, no âmbito do CFMV, a utilização de acessos aos serviços de tecnologia da informação, envolvendo a intranet, internet, extranet, serviços de correio eletrônico (e-mails), hardwares e softwares.

Art. 2º As normas regulamentares são as constantes da Política de Segurança em anexo.

Parágrafo Único. As normas referidas no caput deste artigo serão disponibilizadas na intranet e a qualquer usuário que a solicite.

Art. 3º Dê-se ciência a todos os usuários, bem como ao Departamento de Gestão da Informação, responsável pela gestão da Tecnologia da Informação, para as providências que o assunto requer

Art. 4º Esta Portaria entra em vigor nesta data, revogadas as disposições em contrário.

Gabinete da Presidência, em Brasília-DF, aos vinte e seis dias do mês de dezembro de dois mil e seis.

Méd.Vet. Benedito Fortes de Arruda
Presidente
CRMV/GO Nº 0272

ANEXO

NORMA E POLÍTICA DE ACESSO A INTERNET E UTILIZAÇÃO DE CORREIO ELETRÔNICO

INTRODUÇÃO

Considerando a otimização nas comunicações internas e externas e buscando a diminuição dos gastos com correio convencional e contas telefônicas, o CFMV implanta sua política de acesso à internet e correio eletrônico. Institui com esta política, normas para aplicação em toda a rede, equipamentos e internet, priorizando a segurança das informações e delimitando a conduta dos usuários.

Esta política se aplica a todo usuário que tenha acesso à rede e faça uso da internet ou correio eletrônico, a saber: funcionários efetivos, de livre provimento, comissionados, membros com mandatos eletivos, terceirizados, colaboradores, membros de comissões, entre outros usuários.

A segurança efetiva é um processo que envolve esforço e participação de todos os funcionários do CFMV que lidam com informação. É responsabilidade de todo e qualquer usuário de computador ter conhecimento dessas orientações, conduzindo suas atividade de acordo.

Com fundamento no poder diretivo conferido pela CLT em seu art.2º, o CFMV, estabelece uma política pública sobre o uso da rede e dos meios de informática no local de trabalho. Esta política, que é uma norma coletiva, cientifica os empregados de que a rede, o equipamento, o nome de usuário e a senha que usam são de propriedade do Conselho e que seu tráfego é continuamente monitorado, como também explicita o que será aceito ou não como conduta nas comunicações eletrônicas, suas responsabilidades e deveres quanto ao sigilo dos dados e documentos que manipulam ou têm acesso.

O CFMV utilizará todos os recursos disponíveis e ao seu alcance para divulgar o conteúdo desta Política.

DEFINIÇÕES

Política de Segurança – Conjunto de regras que os funcionários do CFMV devem obedecer no que se refere ao uso dos computadores.

Provedor – Conjunto de computadores e serviços de informática que permitem o acesso a internet.

Rede – Estrutura utilizada para realizar a comunicação entre computadores.

Usuário – Pessoa que está utilizando o computador.

Internet – Rede de computadores mundial

Intranet – Conjunto de serviços, disponibilizados pelo navegador de internet, de maneira restrita a um órgão ou empresa.

Correio Eletrônico – O mesmo que e-mail

Site – Conjunto de páginas da internet.

Vírus – Programa de computador que pode atrapalhar o funcionamento dos softwares ou até mesmo estragar, levando o usuário a perder suas informações.

Spam – E-mails enviados para destinatários que não interessam pelo assunto. Normalmente caracteriza-se por propagandas e correntes, mas dentro de um ambiente corporativo pode aparecer como e-mails de informações que não dizem respeito à pessoa que está recebendo.

Destinatários – Pessoa para a qual se envia uma mensagem.

Software – Programas utilizados nos computadores, ex: word, windows, sistema de cadastro.

Hardware – Equipamento fisico. O computador e suas partes integrantes. Todo equipamento físico utilizado para a geração/manipulação de informação.

Instant Messenger – Mensagens que são enviadas e recebidas de maneira instantânea. Dentro do CFMV, na presente data, este tipo de serviço é provido pelo programa MessagePopup II.

Upload – consiste na ação de enviar arquivos, programas ou qualquer conteúdo para a internet.

Streaming - tecnologia que permite visualizar vídeos, ouvir música, ou outros serviços multimídia sem realizar download.

DO ACESSO À REDE, INTRANET E INTERNET

Terão acesso à rede, intranet e internet, todos os empregados efetivos, de livre provimento, comissionados, terceirizados e que tenham mandato eletivo.

O acesso será possível mediante o cadastro de senhas individuais e sigilosas.

Para ser cliente de navegação, será obrigatória a utilização de software homologado pelo departamento técnico.

DAS SENHAS

Uma senha segura deverá conter no mínimo 6 caracteres alfanuméricos (letras e números) com diferentes caixas. Para facilitar a memorização das senhas, utilize padrões mnemônicos. Por exemplo:

- eSus6C (eu SEMPRE uso seis 6 CARACTERES);
- 9SSgianc (9 Senhas Seguras garantem integridade a nossa organização);
- s3Nh45 (palavra senhas onde o 3 substitui o E, o 4 o A e o 5 o S).

As senhas terão um tempo de vida útil pré-determinado pela equipe de segurança, devendo o mesmo ser respeitado; caso contrário o usuário ficará sem acesso. O usuário deverá trocar a senha a cada 90 (noventa) dias. O próprio sistema irá informar o momento de trocar a senha.

Todas as senhas serão testadas pela equipe de segurança em busca de fragilidades.

O usuário deverá fazer um uso diligente das Contas de Acesso, assim como mantê-las em segredo. Deverá comunicar, imediatamente, à área de informática do CFMV, a perda ou roubo da senha da conta de acesso, assim como qualquer risco de acesso às mesmas por um terceiro.

LEMBRE-SE:

- Sua senha não deve jamais ser passada a ninguém, nem mesmo à equipe de segurança. Caso desconfie que sua senha não esteja mais segura, sinta-se à vontade para mudá-la, mesmo antes do prazo determinado de validade;

- Tudo que for executado com a sua senha será de sua inteira responsabilidade; por isso, tome todas as precauções possíveis para mantê-la secreta.

DO USO DA REDE, INTRANET, INTERNET E EQUIPAMENTOS

O uso da rede, intranet , internet e equipamentos será monitorado constantemente, podendo o usuário prestar contas de seu uso.

O Chefe da Unidade deverá comunicar ao Departamento de Gestão da Informação – DEGIN toda e qualquer movimentação do empregado a ele subordinado, inclusive o afastamento temporário ou permanente, para que as permissões de acesso à internet e e-mails sejam retiradas.

DO CORREIO ELETRÔNICO

O uso do correio eletrônico exige o fornecimento do nome de usuário ou conta e a senha de acesso, que chamaremos de modo conjunto de "Conta de Acesso", fornecidos pela área de informática do CFMV às áreas cujas atividades demandarem a necessidade de uma conta específica.

O correio eletrônico tem caráter exclusivamente funcional. Não será permitido, em caso algum, o seu uso para fins particulares.

O CFMV poderá enviar para a caixa postal dos usuários do serviço de correio eletrônico, mensagens e comunicações de cunho institucional, técnicas e informativos acerca do serviço e demais atividades realizadas no Conselho. A área de informática do CFMV, ao seu exclusivo critério, poderá inserir um complemento (que trate de responsabilidades, avisos, etc.) no "rodapé" das mensagens transmitidas através do serviço.

A inclusão de complementos no rodapé das mensagens não constituirá violação da privacidade das comunicações do usuário, em virtude de ser realizada mediante tratamento automatizado, sem qualquer intervenção humana ou acesso ao conteúdo da mensagem transmitida.

1 - LIMITES DE CAPACIDADE E FUNCIONAMENTO DO SERVIÇO DE CORREIO ELETRÔNICO:

É responsabilidade da área de informática do CFMV estipular os limites de utilização do correio eletrônico que se façam necessários para o bom funcionamento do serviço, incluindo, mas não limitando a quantidade de destinatários, tamanho máximo da caixa postal, as mensagens enviadas e os tipos permitidos de arquivos anexados às mensagens.

2 - TAMANHO DAS CAIXAS POSTAIS:

O tamanho máximo de cada caixa postal será definido pelo provedor de internet em conjunto com a Administração do CFMV, respaldada pela área de informática, considerando a demanda das atividades e a necessidade

do usuário.

3 - TAMANHO DAS MENSAGENS:

O tamanho máximo de cada mensagem será compatível com o tamanho da caixa do usuário.

4 - NÚMERO DE DESTINATÁRIOS:

O número máximo de destinatários simultâneos não tem restrição.

5 - TIPOS DE ARQUIVOS QUE PODERÃO SER ANEXADOS:

Poderão ser anexados os arquivos que contenham documentos, apresentações, planilhas eletrônicas e de banco de dados, que contenham as seguintes extensões:

- Documento: txt; doc; pdf; rtf;
- Apresentação: ppt; pps;
- Planilha eletrônica: xls;
- Banco de dados: mdb;
- Os arquivos supracitados quando compactados: zip.

6 - O QUE É PERMITIDO NO USO DO CORREIO ELETRÔNICO:

- Encaminhar e receber mensagens com assuntos institucionais;
- Anexar mensagens de correio eletrônico arquivos de documentos, apresentações, planilhas eletrônicas e de banco de dados de forma cautelosa, vigiada e orientada.

7 - O QUE É PROIBIDO NO USO DO CORREIO ELETRÔNICO:

- O uso do correio eletrônico para fins particulares;
- A divulgação de informações confidenciais do CFMV 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;
- Enviar ou retransmitir mensagens com conteúdo difamatório, ofensivo, racista ou obsceno,
- Enviar ou retransmitir informação confidencial sem a autorização do CFMV;
- Copiar ou retransmitir mensagens protegidas por direitos específicos

(autorias, propriedade intelectual, etc.) sem permissão do CFMV;

- Transmitir mensagens com conteúdo sexual, racial, político ou religioso (ofensivas ou não), bem como mensagens agressivas ou difamatórias;
- O assédio ou perturbação de outrem, seja através de linguagem utilizada, freqüência ou tamanho das mensagens;
- O envio de e-mail a qualquer pessoa que não o deseje receber. Se o destinatário solicitar a interrupção de envio de e-mails, o usuário deverá acatar tal solicitação e não lhe enviar qualquer mensagem;
- O envio de grande quantidade de mensagens de e-mail ("junk mail" ou "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, propaganda política;
- O envio de e-mails mal-intencionados, tais como "mail bombing" ou sobrecarregar um usuário, site ou servidor com e-mail muito extenso ou numerosas partes de e-mail;
- Forjar qualquer das informações do cabeçalho do remetente;
- A má utilização da linguagem em respostas aos e-mails comerciais, tais como abreviações de palavras (Ex.: “vc” ao invés de “você”);
- Enviar mensagens de correio eletrônico não solicitadas e consentidas previamente, incluindo o envio de mensagem com lixo (junk mail) ou material de propaganda para pessoas que não tenham especificamente solicitado tal material (email spam);
- Solicitar mensagem para qualquer outro endereço de correio eletrônico que não seja o do remetente, com a intenção de coletar respostas;
- Criar ou retransmitir "correntes" ou qualquer outra transmissão em escala;
- Postar mensagens não relacionadas ao trabalho para grande quantidade de grupos de notícias (newsgroup spam);
- Fazer ofertas fraudulentas de produtos ou serviços.

Ao usuário é proibido utilizar o serviço com a finalidade de armazenar, distribuir, transmitir, difundir ou colocar a disposição de terceiros, qualquer classe de conteúdo e, em geral, qualquer classe de material que por si mesmo ou cuja transmissão:

- Contravenha, menospreze ou atente contra os direitos fundamentais e liberdades públicas e individuais, reconhecidas constitucionalmente nos tratados internacionais e no resto do ordenamento jurídico;
- Induza, incite ou promova atuações delituosas, difamatórias, infamantes, violentas, degradantes ou, em geral, contrárias à ordem pública, à lei, à moral e aos bons costumes;
- Induza, incite ou promova atuações, atitudes ou idéias discriminatórias em razão de sexo, raça, religião, crenças, idade ou condição social;
- Incorpore mensagens delituosas, violentas, degradantes ou, em geral,

contrárias à lei, à moral e aos bons costumes ou à ordem pública;
- Induza ou possa induzir a um estado de ansiedade ou temor ou que constituam ameaça ou chantagem a terceiros;
- Induza ou incite práticas perigosas, de risco ou nocivas à saúde e ao equilíbrio psíquico;
- Seja falso, ambíguo, inexato, exagerado ou extemporâneo, de forma que possa induzir a erro sobre o seu objeto ou sobre as intenções ou propósitos do comunicador;
- Esteja protegida por qualquer direito de propriedade intelectual ou industrial pertencente a terceiros, sem que o usuário tenha obtido previamente do seu titular a autorização necessária para realizar o uso a que destina ou a que pretende destinar;
- Viole os segredos empresariais ou institucionais de terceiros;
- Seja contrária ao direito, à honra, à intimidade pessoal e familiar ou à própria imagem das pessoas;
- Infrinja as normas sobre segredo das comunicações;
- Constitua, se for o caso, publicidade ilícita ou enganosa e, em geral, que constitua concorrência desleal;
- Provoque, por suas características (tais como formato, extensão, etc.), dificuldades no normal funcionamento do serviço.

8 - PRÁTICAS NECESSÁRIAS NO USO DO CORREIO ELETRÔNICO:

Grande parte de nossa 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. Devemos lembrar que os vírus atuais são mandados automaticamente. Isso significa que um e-mail de um cliente, parceiro ou amigo NÃO FOI MANDADO NECESSARIAMENTE PELO MESMO.

Nossos servidores de e-mails encontram-se protegidos contra vírus e códigos maliciosos, contudo algumas atitudes são necessárias, dentre outras:

- Não abrir anexos com as extensões (.bat, .exe, .src, .lnk e .com) se não tiver certeza absoluta de que solicitou esse e-mail;
- Desconfiar de todos os e-mails com assuntos estranhos ou em inglês. Alguns dos vírus mais terríveis dos últimos anos tinham assuntos como: I LOVE YOU, Branca de Neve Pornô, etc.;
- Não reenviar e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, criança desaparecida, criança doente, pague menos em alguma coisa, não pague alguma coisa, etc.;
- Não mandar e-mails para mais de 10 pessoas de uma única vez (to, cc, bcc). Trata-se de uma orientação para que seja evitado o spam. Contudo quando for necessário enviar mensagem para todos os CRMVs, faculdades, funcionários, etc, o recurso pode ser utilizado sem limitações.
- Evitar anexos muito grandes;

- Utilizar sempre sua assinatura criptográfica, se disponível, para troca interna de e-mails e quando necessário, para os e-mails externos;
- Escrever as mensagens de maneira clara e objetiva;
- Assinar as mensagens com nome, cargo e unidade do remetente, além do nome da instituição (Conselho Federal de Medicina Veterinária);
- Escrever as mensagens em português, usando as regras de pontuação e ortografia da língua portuguesa (letras maiúsculas no início das frases, nomes próprios, etc.);
- Verificar a ortografia antes da transmissão;
- Só retransmitir mensagens para destinatários que tenham real interesse nelas;
- Ao retransmitir mensagens, colocar claramente que atitude o destinatário deve tomar ao recebê-la;
- Marcar as mensagens como importantes ou urgentes se realmente apresentarem esta condição;
- Apagar as mensagens que já tenham sido lidas e não sejam mais necessárias;
- Não colocar informação confidencial no título, mas dentro do corpo da mensagem em texto claro;
- Afirmar se a opinião é própria em caso de mensagens com endereço eletrônico do CFMV, postadas por usuários em listas ou grupos de discussão, a menos que se trate de atividade decorrente de obrigação funcional.
- Os empregados e terceiros autorizados não devem abrir arquivos anexados a mensagens diferentes dos descritos no item ou acrescido das páginas Web (htm e html), em especial com as extensões .pps e .doc, que são suspeitos de vírus.
- Os empregados e terceiros autorizados devem repassar à unidade gestora dos recursos de informação, mensagens recebidas que possam representar ameaça à segurança da informação do CFMV em função da possibilidade de contaminação por vírus de computador. São características dessas mensagens, dentre outras: remetente desconhecido e assunto não referente aos interesses de trabalho.
- Os empregados e terceiros autorizados devem excluir de suas caixas postais as mensagens recebidas e enviadas que não tenham mais utilidade para o desenvolvimento de suas atividades profissionais, no máximo a cada 90 (noventa) dias.
- Todos os usuários de Internet e correio eletrônico deverão ser bem orientados quanto aos procedimentos em relação aos tipos de arquivos suspeitos (.exe, .doc, .pps, .com, .bat, etc). Em alguns casos esses arquivos deverão ser excluídos e em outros, deverão ser investigados por antivírus para que possam ser utilizados no trabalho. Todos os arquivos passam por antivírus. Contudo, arquivos .exe, .bat, .com, .inf e outros são pequenos programas que podem executar ações malignas ao computador e por isto, o antivírus nem sempre consegue identificar o vírus. O melhor para este

tipo de arquivo é rejeitá-lo. Cabe esclarecer que arquivos do office não devem estar inclusos na lista de arquivos que devem ser rejeitados, contudo necessitam de atenção. Sempre que necessário consultar a área de informática.

- Os usuários devem ser orientados sobre e-mails suspeitos, como exemplo: nome de quem enviou, assunto em inglês, links nos e-mails e outros tipos de arquivos existentes.
- A cota máxima de e-mails armazenados não deve ultrapassar 250 Mega Bytes.

9 - DAS MEDIDAS DE SEGURANÇA:

Caso o CFMV julgue necessário haverá bloqueios:

- De mensagens com arquivos anexos que comprometam o uso de banda ou perturbem o bom andamento dos trabalhos;
- De mensagens para destinatários ou domínios que comprometam o uso de banda ou perturbem o bom andamento dos trabalhos;
- De arquivos ou domínios que comprometam o uso de banda ou perturbem o bom andamento dos trabalhos;

10 - DAS OBRIGAÇÕES DOS USUÁRIOS:

São obrigatórios os seguintes procedimentos:

- Manutenção da caixa de entrada de e-mails, evitando acúmulo de mensagens e arquivos inúteis, a cada 90 dias;
- Utilização de assinatura nos e-mails com o seguinte formato: nome do funcionário, função, matrícula e telefone comercial.
- A manutenção do catálogo de endereços, bem como o backup de e-mails de pastas específicas que não estejam no servidor é obrigação do usuário.

DA REDE DE EQUIPAMENTOS INTERLIGADOS

O objetivo é prestar aos empregados do Conselho Federal de Medicina Veterinária serviços de rede de alta qualidade e ao mesmo tempo desenvolver um comportamento extremamente ético e profissional. Nos termos da Política de Utilização da Rede, o CFMV procederá ao bloqueio do acesso ou o cancelamento do usuário caso seja detectado uso em inconformidades com o aqui estabelecido ou de forma prejudicial à Rede.

O uso da rede engloba desde o “login”, até o uso das impressoras.

É obrigatória a utilização de software homologado pelo departamento técnico.

ESTAÇÕES DE TRABALHO

Cada estação de trabalho tem códigos internos que permitem sua identificação na rede. Como cada funcionário possui sua própria estação de trabalho, significa que tudo que venha a ser executado de sua estação é de responsabilidade do usuário.

1 - PRÁTICAS NECESSÁRIAS NO USO DA ESTAÇÃO DE TRABALHO:

A estação é uma ferramenta de trabalho e também um importante componente de segurança. Sendo assim, algumas práticas devem ser observadas no seu uso, como:

- Manter na estação de trabalho somente o que for pessoal. Todos os dados relativos ao CFMV devem ser mantidos no servidor, onde existe um sistema de backup diário e confiável. Se o usuário não souber como proceder, deverá entrar em contato com a equipe técnica;
- Fechar todos os programas acessados e efetuar o logout/logoff da rede ou bloqueio do desktop através de senha, toda vez que se ausentar do local de trabalho, evitando, desta maneira, o acesso por pessoas não autorizadas;
- Fazer a manutenção no diretório pessoal, evitando acúmulo de arquivos inúteis;
- É prática obrigatória armazenar os arquivos inerentes ao CFMV no servidor de arquivos para garantir o backup dos mesmos;
- Haverá limpeza semanal dos arquivos armazenados na pasta “ARQUIVOS1” ou similar, para que não haja acúmulo desnecessário de arquivos;

2 - O QUE É PROIBIDO:

- Instalar qualquer tipo de software/hardware sem autorização da equipe técnica ou de segurança;
- Usar a estação para baixar ou armazenar MP3, filmes, fotos e softwares com direitos autorais ou qualquer outro tipo de pirataria;
- Qualquer tentativa de obter acesso não autorizado, tais como fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta (também conhecido como "cracking"). Incluído o acesso aos dados não disponíveis para o usuário e a conexão a servidor ou conta cujo acesso não seja expressamente autorizado ao usuário; ou ainda, colocar à prova a segurança de outras redes;
- Qualquer tentativa de interferir nos serviços de outro usuário, servidor ou rede, incluindo ataques do tipo "negativa de acesso", provocando congestionamento em redes;
- Qualquer tentativa deliberada de sobrecarregar ou "quebrar" (invadir) um servidor;
- O uso de qualquer tipo de programa ou comando designado a interferir

com sessão de usuários;

- A exposição, o armazenamento, a distribuição, a edição ou gravação através do uso dos recursos computacionais da rede, de material de natureza pornográfica e racista;
- A criação e/ou remoção de arquivos fora da área alocada ao usuário que venha a comprometer o desempenho e funcionamento do sistema. O compartilhamento de arquivos somente será permitido dentro de um mesmo departamento;
- A utilização da pasta "ARQUIVOS1" ou similar, para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza sensível. Sensíveis são os conteúdos que devem ficar restrito a um grupo ou uma área e não podem ser de conhecimento público. Não chega a ser sigiloso, mas requer uma atenção e cuidado. É bom ressaltar, NÃO deve ser utilizada a pasta arquivos1 ou similar para estes conteúdos.
- A instalação ou remoção de softwares que não forem devidamente acompanhadas pelo Departamento de Gestão da Informação - DEGIN, através de solicitação escrita que será disponibilizada;
- A abertura de computadores para qualquer tipo de reparo. Caso seja necessário, o reparo deverá ser realizado pelo departamento técnico;
- A alteração das configurações da rede e inicialização de máquinas bem como modificações que possam trazer algum problema futuro;
- O uso da rede para atividades ilegais ou que interfiram com o trabalho de outros (interna ou externamente)
- O uso dos equipamentos da empresa para conseguir acesso não autorizado a qualquer outro computador, rede, banco de dados ou informação guardada eletronicamente (interna ou externamente);

DA INTRANET E INTERNET

A Intranet tem por finalidade o uso da tecnologia da internet dentro de uma organização para comunicação, transferência e acesso de dados entre suas unidades, filiais ou sucursais.

A implantação da intranet no CFMV objetiva compartilhar informações, dados e comunicações internas de forma segura e reservada, podendo ser disponibilizado informações e documentos comuns a todas as áreas, como organograma, agenda, rotinas de atividades, acordos coletivos, plano de carreira, cargos e salários, eventos internos, entre diversos outros.

1 - O QUE É PERMITIDO:

- Somente navegação de sites é permitida. Casos específicos que exijam outros protocolos deverão ser solicitados diretamente à equipe de segurança com prévia autorização da chefia local;

- O uso da internet para atividades não relacionadas com os negócios durante o horário de almoço, ou fora do expediente, desde que dentro das regras de uso definidas nesta política;
- Baixar programas ligados diretamente às atividades do CFMV com a devida regularização de suas licença e de seus registros.

2 - O QUE É PROIBIDO:

- O uso da internet para fins particulares ou recreativos durante o horário de expediente;
- Acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados;
- O uso de IM (Instant messengers) não homologados/autorizados pela equipe de segurança;
- Utilizar os recursos do CFMV para fazer o download ou distribuição de software ou dados não legalizados;
- Efetuar "upload" de qualquer software licenciado ao CFMV ou de dados de propriedade do CFMV ou de seus clientes, sem expressa autorização do gerente responsável pelo software ou pelos dados;
- A instalação e uso de softwares de comunicação instantânea, tais como ICQ, Microsoft Messenger e afins;
- A utilização de softwares de peer-to-peer (P2P), tais como Kazaa, Morpheus e afins;
- A utilização de serviços de streaming, tais como Rádios On-Line, Usina do Som e afins.

DAS IMPRESSORAS

1 - PRÁTICAS NECESSÁRIAS NO USO DAS IMPRESSORAS:

- Ao mandar imprimir, verifique na impressora se o que foi solicitado já está impresso. Há várias impressões "sem dono" acumulando-se;
- Se a impressão deu errado e o papel pode ser reaproveitado na sua próxima tentativa, recoloque-o na bandeja de impressão. Se o papel servir para rascunho, leve-o para sua mesa. Se o papel não servir para mais nada, jogue-o no lixo;
- Não deixe impressões erradas na mesa das impressoras, na mesa das pessoas próximas a ela e tampouco sobre o gaveteiro;
- Se a impressora emitir alguma folha em branco, recoloque-a na bandeja;
- Se notar que o papel de alguma das impressoras está no final, faça a gentileza de reabastecê-la. Isto evita que você e outras pessoas tenham seus pedidos de impressão prejudicados e também o acúmulo de trabalhos

na fila de impressão;
- Utilize a impressora colorida somente para versão final de trabalhos e não para testes ou rascunhos.

DO MONITORAMENTO

Como o CFMV disponibiliza o uso do correio eletrônico para assuntos estritamente institucionais, o conteúdo das mensagens poderá ser rastreado ou varrido por processos automáticos (softwares especiais) ou semi-automáticos, com o intuito de verificar a obtenção, retenção, uso e divulgação de informações por meios ou com fins ilícitos e em desacordo com as regras desta Política, assim como detectar a presença de vírus ou código executável nocivo à rede, podendo retê-las ou bloqueá-las temporária ou definitivamente, como por exemplo: acesso ao e-mail dependendo do problema detectado. Contudo, estes procedimentos serão tomados, sempre com aval do Secretário-Geral e/ou da Presidência do Conselho.

É proibido a qualquer usuário monitorar, interceptar, editar, acessar e/ou divulgar informações relativas a outro usuário ou ao conteúdo de suas comunicações privativas. Esta proibição se estende, inclusive, aos administradores da rede e do serviço de correio eletrônico, salvo nas hipóteses previstas na Política de Segurança da Informação do CFMV e na legislação em vigor para atender à demanda judicial, investigação administrativa ou policial devidamente justificadas.

Devido à natureza das comunicações eletrônicas e da tecnologia empregada, o CFMV não pode garantir de forma absoluta a privacidade na utilização do serviço por parte dos usuários e, em particular, não pode garantir que terceiros não autorizados não possam acessar e, eventualmente, interceptar, eliminar, alterar, modificar ou manipular de qualquer modo o conteúdo disponibilizado através do serviço ou interceptar, eliminar, alterar, modificar ou manipular de qualquer modo os arquivos e comunicações de qualquer classe que os usuários transmitam, armazenem ou ponham à disposição de terceiros através do serviço, embora o CFMV utilize todos os esforços e recursos tecnológicos e humanos à sua disposição para evitar que tais fatos aconteçam.

O CFMV poderá gerar relatórios dos sites acessados por qualquer usuário e, se necessário, poderá publicar essas informações.

DA RESPONSABILIDADE CIVIL

O usuário deve utilizar o serviço em conformidade com a lei, a moral, os bons costumes e a ordem pública, de forma adequada e diligente, assim

como se abster de utilizá-lo com objetivos ou meios para a prática de atos ilícitos, proibidos pela presente política ou pelas demais normas do CFMV, assim considerados: atos lesivos aos direitos e interesses de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar o serviço e a rede do CFMV ("vírus", arquivos do tipo "cavalo de tróia", "correntes - chain letters", etc.).

São também considerados atos lesivos, os que de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os equipamentos informáticos de outros usuários (hardware e software), assim como os documentos, arquivos e toda classe de conteúdos armazenados nos seus equipamentos informáticos ou impedir a normal utilização ou gozo do referido serviço.

É importante que todos os usuários do serviço de Correio Eletrônico estejam cientes dos riscos legais envolvendo seu uso.

O usuário que, por ato ilícito, causar dano a outrem, fica obrigado a repará-lo, nos moldes do art. 927 do Código Civil.

DAS SANÇÕES

O empregado que violar qualquer item desta norma está sujeito à instauração de sindicância e abertura de processo administrativo disciplinar, procedimentos estes previstos na legislação em vigor e normas do CFMV, podendo ensejar, de acordo com a infração cometida as seguintes sanções:

1 - ADVERTÊNCIA OU SUSPENSÃO:

A pena de advertência ou suspensão será aplicada, por escrito, somente nos casos de infrações de menor gravidade.

2 - DEMISSÃO POR JUSTA CAUSA:

Aplicar-se-á a pena de demissão por justa causa nas hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho.

Fica desde já estabelecido que não há progressividade como requisito para a configuração da dispensa por justa causa, podendo o CFMV, no uso do seu poder diretivo e disciplinar, aplicar a pena que entender devida quando tipificada a falta grave.

Será encaminhado ao empregado, comunicado informando o

descumprimento da norma, com a indicação precisa da violação praticada. Cópia desse comunicado permanecerá arquivada junto a área de Recursos Humanos na respectiva pasta funcional do infrator.

DISPOSIÇÕES FINAIS

Para resguardar a política de segurança algumas medidas devem ser observadas, tais como:

- Não fale sobre a política de segurança da CFMV com terceiros ou em locais públicos;
- Não diga sua senha para ninguém. Nossa equipe técnica jamais irá pedir sua senha;
- Não digite suas senhas ou usuários em máquinas de terceiros, especialmente fora do CFMV;
- Somente aceite ajuda de um membro de nossa equipe técnica previamente apresentado e identificado;
- Nunca execute procedimentos técnicos cujas instruções tenham chegado por e-mail;
- Relate à equipe de segurança, pedidos externos ou internos que venham a discordar dos tópicos anteriores;
- Mantenha seu antivírus atualizado. Provavelmente nossa equipe técnica irá se encarregar disso, mas caso não tenha sido feito ou você perceba que a atualização não está funcional, entre em contato com a mesma para que a situação possa ser corrigida;
- Não traga disquetes, CDs ou “opendrives” de fora do CFMV. Caso isso seja extremamente necessário, encaminhe o mesmo para a equipe técnica, onde passará por uma descontaminação;
- Reporte atitudes suspeitas em seu sistema à equipe técnica, para que possíveis vírus possam ser identificados no menor espaço de tempo possível;
- Suspeite de softwares que "você clica e não acontece nada".

Para garantir as regras mencionadas acima o CFMV se reserva no direito de:

- Implantar softwares e sistemas que podem monitorar e gravar todos os usos de Internet através da rede e das estações de trabalho do CFMV;
- Inspecionar qualquer arquivo armazenado na rede que esteja no disco local da estação ou nas áreas privadas da rede, visando assegurar o rígido cumprimento desta política;
- Instalar softwares e hardwares para proteger a rede interna e garantir a integridade dos dados e programas, incluindo um firewall, que é a

primeira, mas não a única barreira entre a rede interna e a Internet.

De nada adianta uma informação segura se a mesma estiver indisponível para quem necessita dela. Por isso o Conselho Federal de Medicina Veterinária e sua equipe de segurança contam com a colaboração de todos na conscientização de que a informação é um ativo que, como qualquer outro, é importante para organizações e negócios, tem um valor para o CFMV e, conseqüentemente, necessita ser adequadamente protegida.

A política de segurança protege a informação de diversos tipos de ameaça, para garantir a continuidade dos negócios, minimizando os danos a eles e maximizando o retorno dos investimentos e as oportunidades de negócio.

A informação pode existir em muitas formas: pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que seja protegida adequadamente.

Todos os usuários devem seguir as regras e orientações desta Política, de forma a garantir o uso apropriado e eficiente do serviço, reduzindo as possibilidades não só dos eventos citados acima, mas de qualquer ocorrência que possa comprometer a segurança da rede e imagem do CFMV.

Este documento tem a intenção de estabelecer regras, limites e controles, com o fito de proteger, salvar e guardar as informações e os interesses do CFMV.

Brasília – DF, 27 de novembro de 2006.

Elaboração:

Assessoria de Gestão e Planejamento – AGESP
Departamento de Gestão da Informação – DEGIN

Validação:
Assessoria Jurídica – ASJUR
Secretário-Geral do CFMV

APÊNDICE I

TERMO DE COMPROMISSO E RESPONSABILIDADE INDIVIDUAL

Declaro, sob as penas da lei, ter conhecimento das normas de utilização e acesso à rede, internet, intranet e correio eletrônico do Conselho Federal de Medicina Veterinária – CFMV.

Declaro, outrossim, que assumo toda e qualquer responsabilidade por eventuais problemas decorrentes de acessos indevidos à internet ou de utilização imprópria da conta de e-mail: ....., disponibilizada para uso no desempenho de minhas atribuições, e que estarão sujeitos a fiscalização e controle da administração do Conselho.

Em cumprimento às normas deste órgão, para todos os efeitos legais, assino o presente termo de compromisso e responsabilidade, em duas vias, de igual forma e teor, uma das quais passará a integrar o acervo documental do CFMV.

Brasília – DF, ...

Nome/cargo/função

APÊNDICE II

TERMO DE AUTORIZAÇÃO E RESPONSABILIDADE

Autorizo a liberação de acesso a internet ao(s) empregado(s) abaixo nominado(s) e lotado(s) nesta Unidade, para utilização no desempenho de suas atribuições, observada a Política de Segurança implantada no CFMV e o Termo de Responsabilidade assinado pelo usuário.

Autorizo também, a criação de uma conta de e-mail de uso institucional para o(s) empregado(s) abaixo nominado(s) e lotado(s) nesta Unidade, para o desempenho de suas atribuições, nos termos da Política de Segurança implantada nesta Casa e o Termo de Responsabilidade assinado pelo usuário.

Desta forma, declaro, sob as penas da lei, ter conhecimento das normas de utilização e acesso à internet, bem como da política de e-mails do Conselho Federal de Medicina Veterinária – CFMV e assumo o compromisso de orientar e monitorar os acessos realizados pelo(s) referido(s) empregado(s).

Declaro ainda, que todo e qualquer fato ou problema decorrentes de acessos indevidos à internet ou de utilização imprópria da conta de e-mail do(s) empregado(s) lotado(s) nesta Unidade será comunicado ao Departamento de Gestão da Informação – DEGIN, com a indicação das providências pertinentes, inclusive no caso de afastamento temporário ou definitivo do empregado, para que seja bloqueado o acesso.

Em cumprimento às normas do CFMV, para efeitos legais, assino o presente termo, em duas vias, de igual forma e teor.

Brasília – DF, ...

Nome/cargo/função