Fatec Jundiaí

PORTARIA FATEC / JUNDIAÍ Nº 04/2010 DE 28 DE JULHO DE 2.010

Estabelece Normas Internas para Segurança de Informações

O Diretor da Faculdade de Tecnologia de Jundiaí, no uso de suas atribuições legais, estabelece o seguinte:

Artigo1° - Objetivo

Está portaria estabelece e define as diretrizes para gestão de segurança da Faculdade de Tecnologia de Jundiaí, e, em conformidade com a NBR ISO/IEC 27002:2005 e PRODESP, visa garantir:

Confidencialidade: Garantia do limite de acesso à informação somente por pessoas autorizadas;

Integridade: Segurança de que as informações mantenham todas as características originais e sejam alteradas somente por meio de ações planejadas e autorizadas;

Disponibilidade: Garantia de que os usuários autorizados tenham acesso à informação da instituição.

Descreve, ainda, a conduta adequada dos servidores, alunos e professores para a segurança, controle, proteção, utilização, divulgação, autorização, destruição, e modificação das informações confidenciais e internas da Fatec Jundiaí.

Artigo 2° - Política

Parágrafo 1º - Propriedade dos recursos

Os recursos de TI disponibilizados tais como softwares, hardwares, impressoras, copiadoras, discos, etc; utilizados pelos usuários para o desenvolvimento de suas atividades, são de propriedade da Fatec Jundiaí.

Parágrafo 2° - Divulgação de Informações

Parágrafo 2.1 - Engenharia Social

São práticas utilizadas por pessoas mal intencionadas com o desejo de obter acesso às informações confidencias, por meio de convencimento dos servidores, explorando a confiança do usuário, para ter acesso ilegal às informações que não são divulgadas. O procedimento é feito de forma legítima, com a exploração das falhas humanas e não dos Sistemas de Segurança de informação.

A maioria das técnicas de Engenharia Social consistem em obter informações sigilosas, enganando os usuários por meio de identificação falsa, por telefones ou e-mails (arquivos contendo SPAM), ou conversas diretas em locais adversos ao da instituição.

O usuário deve estar ciente do valor das informações que possui e da responsabilidade de proteção, e deve seguir os seguintes preceitos de segurança.

Evitar conversas com outras pessoas sobre assuntos internos a Fatec Jundiaí, confidenciais ou internos, em locais fora do trabalho e/ou na presença de terceiros.

Informações confidenciais ou internas não devem ser disponibilizadas a quaisquer pessoas desconhecidas, ou a quem não esteja diretamente ligado ao assunto.

Adotar sempre uma postura reservada com pessoas que tentarem obter informações confidenciais ou internas da Fatec Jundiaí.

Não divulgar informações da Fatec Jundiaí por telefone às pessoas que não se identificarem.

Parágrafo 2.2 - Manuseio de Documentos Impressos

Qualquer material impresso contendo informações confidenciais ou internas não deve ser descartado em cesto de lixo ou em caixa de material para reciclagem. Deve ser “rasgado” ou ser encaminhado à Diretoria de Serviços para serem triturados.

Não deixar, nas copiadoras ou impressoras, material contendo informações confidenciais ou internas, possibilitando que terceiros se apropriem do material ou tenha acesso indevido às informações.

Não utilizar como rascunho papéis ou documentos contendo informações confidenciais.

Parágrafo 2.3 - Descarte de Mídia

Os diversos tipos de mídias – ótica, magnética e eletrônica – quando não forem mais necessárias, devem ser descartadas de forma segura, através de trituração ou destruição, que não deixem expostos seus conteúdos, por conterem informações sigilosas.

O descarte de discos – rígidos ou magnéticos – devem ser feitos através da equipe de TI da Fatec Jundiaí, órgão competente para formatação física e/ou destruição destas mídias.

Artigo 3° - Acesso a Internet

Baseando-se na norma emitida pela Prodesp, como Administradora da Rede IP Multiserviços, e que se aplica a partir da data de sua publicação no site da INTRAGOV (www.INTRAGOV.sp.gov.br) a todos os órgãos e entidades signatárias do Projeto

INTRAGOV, conforme item “d” da Cláusula segunda (dos compromissos dos Signatários) do Termo de Cooperação celebrado entre as Secretarias do Governo e Gestão Estratégica, Fazenda, Segurança Pública, Economia e Planejamento, Educação, a Imprensa Oficial do Estado de São Paulo – IMESP e a Cia. De Processamento de Dados do Estado de São Paulo – PRODESP, bem como a Cláusula segunda do Termo de Adesão ao Termo de Cooperação, mencionado acima.

Parágrafo 1° - Finalidade desta Norma

Parágrafo 1.1 - Regular o acesso à Internet via Unidade Provedora Internet (UPI) da Rede IP Multisserviços. Este documento contém as instruções que se aplicam aos usuários de recursos da rede local de uma Unidade Cliente (UC) ou de uma Unidade Provedora (UP) disponíveis para esta finalidade;

Parágrafo 1.2 - Atender aos termos e condições do Serviço Acesso Internet, conforme disposto no Contrato PRO.00.4733, às disposições normativas das entidades que disciplinam o uso da Internet, tais como o Comitê Gestor de Internet – Brasil (CGI-br na URL: http://cartilha.cert.br/download/ cartilha- seguranca-internet.pdf) e às normas específicas de controle e segurança de cada órgão do Governo do Estado de São Paulo;

Parágrafo 1.3 - Disciplinar a utilização segura e eficiente dos recursos da Rede I Multisserviços.

Artigo 4° - Utilização da Internet

Parágrafo 1° - O uso da Internet é para fins educacionais e profissionais, este último com objetivo de aumentar a produtividade dos processos de trabalho, visando ao interesse do Estado e ao atendimento do cidadão. . É terminantemente vedado a todos os usuários,

sob pena de sofrer as sanções disciplinares, trabalhistas e legais, sem prejuízo de outras disposições normativas aplicáveis, o disposto a seguir:

- Invadir a privacidade ou a intimidade de terceiros através de ações de busca de senhas ou de dados privativos, de modificação de arquivos ou personificação da identidade de terceiros;

- Dissimular sua identidade através da alteração dos endereços IP a equipamentos da rede local da Unidade ("IP-Spoofing");

- Tentar acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta;

- Executar testes de vulnerabilidade de segurança em redes, servidores ou qualquer outro dispositivo de rede;

- Violar a segurança de qualquer servidor, rede, provedor ou indivíduo;

- Alterar indevidamente dados disponíveis na rede;

- Interferir nos serviços prestados na rede, bem como provocar o congestionamento, proposital ou não, ou cometer ações, deliberadas ou não, que sobrecarreguem um servidor ou serviço disponível;

- Desrespeitar a legislação, de natureza cível ou criminal, aplicável ao Serviço de Acesso à Internet, inclusive referente à segurança, confidencialidade e propriedade intelectual;

- Permitir, facilitar ou incitar, direta ou indiretamente, o acesso não autorizado de qualquer natureza a computadores ou a redes dos Órgãos Signatários do Projeto INTRAGOV ou de qualquer outra entidade ou organização;

- Por em risco a procedência, autenticidade, integridade ou sigilo das informações ou dados dos Órgãos Signatários do Projeto INTRAGOV ou de terceiros;

- Prejudicar intencionalmente outros usuários, através do desenvolvimento ou disseminação de programas nocivos, conhecidos como malwares (vírus, “cavalos-de-

tróia", worms e outros códigos maliciosos), bem como a utilização de "cookies" em desacordo com as leis ou com as melhores práticas de mercado;

- Interferir nos serviços de qualquer outro usuário, servidor ou rede, incluindo ataques do tipo "negativa de acesso", provocar congestionamento em redes, tentativas deliberadas de sobrecarregar e/ou "quebrar" (invadir) um servidor;

- Expor, armazenar, distribuir, editar ou gravar material de natureza pornográfica, racista ou de conteúdo ilegal ou imoral;

- Fazer o download ou distribuição de software/dados não legalizados;

- Divulgar informações confidenciais ou privadas em grupos de discussão, listas ou outros meios;

- Utilizar softwares de comunicação instantânea, tais como ICQ, chats (bate - papo) e afins, bem como variantes baseadas no navegador;

- Utilização de programas para transferência de arquivos ponto-a-ponto (Peer-to-Peer / P2P);

- Efetuar Upload de qualquer programa (software) licenciado ao Governo ou Instituições Governamentais de dados de propriedade de sua propriedade ou de cidadãos, sem expressa autorização do responsável pelo programa ou pelas informações;

- Autorizar conexões originadas no ambiente externo (Internet) e destinadas ao uso de aplicações residentes em microcomputador ou na rede de microcomputadores da Unidade Cliente. Desta forma, ficam proibidas no ambiente da Unidade Cliente, dentre outras, aplicações de hospedagem de conteúdo para acesso externo, instalação de servidores de página (Web), servidores de e-mail, de Terminal Services, de gerenciamento/manutenção remota ou de transferência de arquivo (FTP ou afins), que sejam acessadas a partir do ambiente externo (Internet).

- Navegar em quaisquer sites cujo conteúdo não seja condizente com a ocupação do usuário, como por exemplo:

- Acesso a sites com conteúdo de fraudes;
- Acesso a sites com conteúdo hacker;
- Acesso a sites com conteúdo pedófilo;
- Acesso a sites com conteúdo racista;
- Acesso a sites com conteúdo terrorista;
- Acesso a sites com conteúdo pornográfico;
- Acesso a sites com conteúdo de jogos;
- Acesso a sites com conteúdos obscenos;
- Acesso a sites de relacionamento pessoal;
- Acesso a sites de troca de mensagens;
- Acesso a sites com conteúdo ilícitos;
- Acesso a sites de apostas.

Artigo 5° - Recomendação de Uso dos Computadores

Parágrafo 1° - A senha de um usuário deve ser pessoal e intransferível, sendo o mesmo responsável pelo seu uso;

Parágrafo 2° - Devem ser utilizadas senhas fortes, com o tamanho de pelo menos 8 dígitos,compostas de letras, números e símbolos;

Parágrafo 3° - A senha deve ser trocada periodicamente;

Parágrafo 4° - Antes de ausentar-se do seu local de trabalho, o usuário deverá fechar todos os programas acessados, evitando, desta maneira, o acesso por pessoas não autorizadas e, sempre que possível, efetuar o "logout/logoff" da rede ou bloqueio do computador através de senha;

Parágrafo 5° - Realizar o "download" somente de programas ligados diretamente às atividades de ensino, de Governo e atendimento ao Cidadão, sendo estes devidamente autorizados pelo responsável pela unidade;

Parágrafo 6° - Para melhoria no desempenho no envio de e-mails, recomenda-se que sejam compactados todos os arquivos anexados a e-mails, principalmente, aqueles com tamanho superior a 1 Megabyte;

Parágrafo 7° - A utilização de serviços de "streaming", tais como rádios e vídeos on-line ocasionam o congestionamento da rede, portanto devem ser evitados.

Artigo 6° - Norma para acesso a Internet e Restrições de Segurança

Parágrafo 1° - O acesso às páginas com conteúdo inadequado, como pornografia, racismo, jogos de azar e outros, são de acesso proibido, exceto nos casos expressamente autorizados por autoridade competente com a finalidade de investigação/ apuração de fatos. Neste último caso, a tentativa e o acesso às paginas de conteúdo proibido serão registrados.

Parágrafo 2° - A critério da Administradora da Rede IP Multisserviços, poderão ocorrer bloqueios de acesso à:

Parágrafo 3° - Arquivos que comprometam a segurança, o desempenho ou a disponibilidade da rede e seus serviços;

Parágrafo 4° - Domínios que comprometam a segurança, o disponibilidade da rede e seus serviços.

Artigo 7º - Desligamento ou Transferência de Alunos e funcionários

Parágrafo Único - Sempre que ocorrer o desligamento ou transferência de um aluno, o fato deverá ser comunicado imediatamente a área de TI, para que os acessos /direitos do usuário sejam revogados. A comunicação deve ser formal, por e-mail, endereçadas aos Administradores do Sistema.

Artigo 8° - Acesso a Rede Wireless

Parágrafo 1° - Somente os alunos regularmente matriculados, professores e colaboradores podem ter acesso a rede wireless. O uso da rede wireless por quaisquer outros usuários (prestadores de serviços, visitantes, parceiros, etc...), deve ser previamente autorizado através de solicitação de um responsável da Instituição;

Parágrafo 2° - O Uso a rede Wireless deve ser criptografado por meio de uso de chave compartilhada (WPA)

Artigo 9° - Esta portaria entra em vigor a partir da data de sua publicação.

Prof. Dr. Antonio Cesar Galhardi
Diretor
Fatec Jundiaí