Política de segurança e de uso das tecnologias de informação

Este documento foi elaborado tomando-se como base o documento “Práticas de Segurança para Administradores de Redes Internet”, disponível em http://www.nbso.nic.br/, adaptado às particularidades da FUPF e suas mantidas.

A política de segurança é um instrumento para proteger a Instituição contra ameaças à segurança da informação que a ela pertence ou que está sob sua responsabilidade. Uma ameaça à segurança é compreendida neste contexto como a quebra de uma ou mais de suas três propriedades fundamentais (confidencialidade, integridade e disponibilidade).

A política de uso é um instrumento que garante a correta utilização dos recursos de tecnologia de informação (TI). Por recursos de TI entende-se: acesso aos sistemas informatizados, utilização dos dados e informações geradas, tratadas e mantidas através dos recursos de informática (*hardware* e *software*), do correio eletrônico, bem como do acesso à Internet, Intranet e outras mídias. O uso indevido caracteriza-se pela violação de direitos autorais, uso de ferramentas ou práticas que prejudiquem a atividade fim da Instituição ou ainda que infrinjam a legislação nacional vigente.

A política de segurança e de uso atribui direitos e responsabilidades aos usuários. Entende-se por usuários: alunos, professores e funcionários da Instituição, bem como outras pessoas que utilizam os recursos de TI da Instituição dentro ou fora da mesma. A política de segurança e de uso também estipula as penalidades às quais estão sujeitos aqueles que a descumprem.

A política de segurança e de uso compreende:

1. Quanto aos aspectos gerais:

   - Abrangência e objetivo de atuação da política: dispõe sobre a política de segurança e uso dos recursos de TI nas dependências da Fundação Universidade de Passo Fundo e suas mantidas.
   - Normas, regulamentos e competências aos quais a política está subordinada: esta política está subordinada ao regimento geral da Instituição bem como à legislação vigente. A responsabilidade de sancionar esta política é de competência da reitoria. Cabe à reitoria o encaminhamento da sanção desta política, ficando a implementação e fiscalização sob responsabilidade dos órgãos executores relacionados às áreas de TI.
   - Meios de distribuição da política: esta política deve ser apresentada aos usuários quando do seu ingresso na Instituição e estará disponível para consulta nos Sistemas Informatizados, na Intranet e na Internet.

- Revisão da política: esta política deverá ser revisada pela Comissão de TI anualmente ou de acordo com os interesses e demandas da Instituição.

2. Quanto aos direitos e responsabilidades dos usuários:

- Contas de acesso: os usuários de recursos de TI terão direito à utilização de contas protegidas por senha e grupos de privilégios, de acordo com sua categoria na Instituição. As categorias juntamente com seus privilégios são divididas em: professores e funcionários (acesso à Intranet, Internet e Sistemas Informatizados), alunos (Intranet e Internet) e outros (de acordo com o interesse e necessidade da Instituição). A proteção e o uso de informações como senhas, dados de configuração de sistemas e dados confidenciais da Instituição são de inteira responsabilidade dos usuários.
- *Softwares*: é permitido aos usuários utilizar, única e exclusivamente, softwares autorizados pela Instituição.
- Informações: é vedado aos usuários, quando da utilização dos recursos de TI da Instituição, infringir a lei de *copyright*.
- Recursos de TI: devem ser utilizados exclusivamente para as atividades fins da Instituição.
- Privacidade de informações: as informações particulares dos usuários poderão ser disponibilizadas somente por determinação judicial ou por interesse da instituição e devem ser garantidas pelo provedor dos recursos (Instituição).
- Antivírus: a utilização e a atualização do antivírus fornecido pela Instituição são de responsabilidade dos usuários.
- *Backups*: é de responsabilidade dos usuários a realização de *backups* (cópias de segurança) de dados e informações armazenados em seu(s) microcomputador(es) de trabalho.

3. Quanto aos direitos e responsabilidades do provedor dos recursos:

- São de inteira responsabilidade da Divisão de Tecnologia de Informações - DTI as seguintes atribuições:
    1. A realização de *backups* dos dados armazenados nos servidores corporativos que mantêm serviços de interesse institucional.
    2. Determinar as diretrizes a serem aplicadas aos serviços necessários para a correta administração da rede da Instituição (configuração e instalação de sistemas e equipamentos de rede e telecomunicação).
    3. Conceder e revogar autorizações de acesso, conectar e desconectar sistemas e equipamentos de rede, alocar e registrar endereços e nomes de sistemas e equipamentos.

4. Monitorar os sistemas e os equipamentos de rede.

- Normas de segurança: devem estar em consonância com as diretrizes estabelecidas pelos setores responsáveis pelas infra-estruturas de informática, de construção predial, de instalações elétricas, de conforto térmico e de segurança patrimonial.

4. Quanto às ações previstas em caso de violação da política de segurança e de uso de TI:

- Diretrizes para tratamento e resposta de incidentes de segurança: quando da ocorrência de incidentes que venham a afetar a segurança e o provimento dos serviços de informática mantidos pela Instituição, caberá à DTI exercer ações necessárias para garantir o bom funcionamento da rede.
- Penalidades cabíveis: as ocorrências de incidentes serão encaminhadas à Comissão de TI que, por sua vez, analisará caso a caso e encaminhará à Reitoria para a aplicação da penalidade indicada para a situação.

Os casos não contemplados neste documento serão analisados pela Comissão de Tecnologia de Informação.