Política de Segurança da Informação - PSI

NORMAS DE APLICAÇÃO

1. Abrangência

A Política de Segurança da Informação da FEU destina-se a todos os gestores, empregados, estagiários e colaboradores da Fundação Editora da Unesp – FEU, doravante denominados Usuários.

Para fins didáticos, esta Política adotará para a Fundação Editora da Unesp – FEU, a nomenclatura técnica de Fundação.

2. Conceito

A Política de Segurança da Informação é um conjunto de procedimentos e orientações a serem seguidos por todos os membros da Fundação, visando proteger o bem mais valioso, a INFORMAÇÃO, qualquer que seja a forma de apresentação podendo ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas.

Seja qual for a forma de apresentação ou meio através do qual e compartilhada ou armazenada é recomendado que ela seja protegida adequadamente. “Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser

estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio."

3. Objetivos

Os principais objetivos da Política de Segurança da Informação – PSI são estabelecer diretrizes que permitam aos empregados, colaboradores e clientes seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e proteção legal da Fundação e do indivíduo:

- Conscientizar os usuários de informação sobre sua segurança e privacidade;
- Definir normas, responsabilidades, obrigações e sanções para todos que tiverem acesso a algum tipo de informação;
- Preservar a corporatividade, a receita, a lucratividade, o atendimento aos requisitos legais e a imagem da Fundação no mercado;
- Proteger e preservar a integridade, confiabilidade e disponibilidade da informação, protegendo e preservando o negócio da Fundação.

Como preservar a integridade? -- Manter sempre a informação na mesma condição disponibilizada por seu proprietário, inserindo, se for o caso, proteção contra alterações, sejam elas intencionais, indevidas ou acidentais.

Como preservar a confiabilidade? – Manter a informação protegida conforme o grau de sigilo e seu conteúdo, inserindo, se for o caso limitação de acessos.

Como preservar a disponibilidade? -- Manter disponível toda informação gerada ou adquirida a seus usuários no momento que necessitem.

4. Responsabilidades

A Fundação Editora da Unesp – FEU entende que o Sistema de Segurança da Informação somente será eficaz com o comprometimento de todos os usuários: gestores, empregados, estagiários e colaboradores.

Dos Usuários em Geral

- Respeitar esta Política de Segurança da Informação;
- Responder pela guarda e proteção dos equipamentos e recursos computacionais colocados à sua disposição para execução de suas tarefas;
- Responder pelo uso exclusivo e intransferível de suas senhas acesso.
- Ativar suas senhas de proteção para Correio Eletrônico e Sistema Operacional, sob orientação do responsável pela área de Tecnologia da Informação – TI;
- Adquirir conhecimento necessário para a correta utilização dos recursos da hardware e software;
- Comunicar prontamente à área de TI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus, etc.;
- Certificar que as informações e dados de propriedade da Fundação não sejam disponibilizados para terceiros, a não ser com autorização, por escrito do superior hierárquico da área de TI;
- Relatar para o seu responsável hierárquico e a área de TI, a necessidade de um novo software para a execução de suas atividades;
- Responder pelo prejuízo ou dano que vier a causar à FEU, ou a terceiros, em decorrência da não obediência as diretrizes e normas aqui expressas.

Dos Gestores de Pessoas e/ou Processos

- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os empregados, estagiários e colaboradores;
- Atribuir aos empregados, estagiários e colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da FEU, mediante assinatura de Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da Fundação;
- Antes de conceder o acesso às informações da FEU a colaboradores eventuais e prestadores de serviços, exigir assinatura do Acordo de Confidencialidade;
- Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI;
- Autorizar o acesso e definir o perfil e mudança de perfil do usuário junto ao responsável pela área de TI;
- Relatar prontamente à área de TI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus, etc.
- Relatar para seu superior hierárquico e a área de TI, o surgimento da necessidade de um novo software para o desenvolvimento de suas atividades.
- Responder pelo prejuízo ou dano que vier a provocar à FEU ou a terceiros, em decorrência da não obediência às diretrizes e normas que expressas.

Dos Detentores da Informação

Da Área de Tecnologia da Informação:

- Testar a eficácia dos controles utilizados e informar aos gestores os riscos existentes;
- Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.
- Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir as exigências de segurança constantes desta PSI.
- Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.
- Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.
- Garantir segurança especial para sistemas com acesso público, incluindo o ambiente educacional, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.
- Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para o FEU.

- Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela área de Tecnologia da Informação - TI, nos ambientes totalmente controlados por ela.
- O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.
- Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.
- Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:
- Os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.
- Os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.
- Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.
- Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.
- Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente

exclusivamente educacional, exigindo o seu cumprimento dentro da empresa.

- Realizar auditorias periódicas de configurações técnicas e análise de riscos.
- Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.
- Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.
- Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.
- No ambiente de TI, gerar indicadores e históricos de:
    - uso da capacidade instalada da rede e dos equipamentos;
    - tempo de resposta no acesso à internet e aos sistemas críticos da FEU;
    - períodos de indisponibilidade no acesso à internet e aos sistemas críticos da FEU;
    - incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
    - atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

Da Área de Segurança da Informação:

- Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.

- Propor e apoiar iniciativas que visem à segurança dos ativos de informação do FEU.
- Publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pela Diretoria Executiva.
- Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio do FEU mediante campanhas, palestras, treinamentos e outros meios de endomarketing.
- Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.
- Analisar criticamente incidentes que possam interferir nas atividades da FEU.
- Apresentar as atas e os resumos das reuniões realizadas pela área de TI, destacando os assuntos que exijam intervenção da própria área ou de membros da Diretoria Executiva.
- Manter comunicação efetiva com a área da TI sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a FEU. Buscar alinhamento com as diretrizes corporativas da instituição.

DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta PSI, a FEU poderá:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação da área de TI ou Diretoria Executiva;

- Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

CORREIO ELETRÔNICO

O objetivo desta norma é informar aos colaboradores da FEU quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico da FEU é para fins corporativo relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a FEU e também não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico da FEU para:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso necessário da FEU;
- Enviar mensagem pelo endereço de sua área ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente a FEU ou unidades vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Apagar mensagens pertinentes de correio eletrônico quando qualquer uma das áreas da FEU estiver sujeita a algum tipo de investigação;

- Produzir, transmitir ou divulgar mensagem que:
    - contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do FEU;
    - contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador; - contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
    - vise obter acesso não autorizado a outro computador, servidor ou rede;
    - vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
    - vise burlar qualquer sistema de segurança;
    - vise vigiar secretamente ou assediar outro usuário;
    - vise acessar informações confidenciais sem explícita autorização do proprietário;
    - vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
    - inclua imagens criptografadas ou de qualquer forma mascaradas;
    - contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet);
    - tenha conteúdo considerado impróprio, obsceno ou ilegal;
    - seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
    - contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
    - tenha fins políticos locais ou do país (propaganda política);
    - inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador
- Gerência ou Área de Trabalho
- Nome da Fundação
- Telefone(s)
- endereço eletrônico

INTERNET

Todas as regras atuais da FEU visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a FEU, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da FEU, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A FEU, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos.

Apenas os colaboradores autorizados pela instituição poderão copiar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades na FEU.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela área de TI.

Os colaboradores não poderão em hipótese alguma utilizar os recursos da FEU para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato) não poderão ser realizados por usuários. que tenham atividades profissionais relacionadas a essas categorias.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado à FEU ou de dados de sua propriedade aos seus

parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os colaboradores não poderão utilizar os recursos da FEU para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores. O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos.

IDENTIFICAÇÃO

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a FEU e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

Todos os dispositivos de identificação como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese. Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a FEU e a legislação (cível e criminal). será dos usuários que dele se utilizarem.

Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado. É proibido o compartilhamento

de login para funções de administração de sistemas. A área de recursos humanos é a responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.

A área de TI responde pela criação da identidade lógica dos colaboradores na instituição. Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas.

Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha de acordo com as orientações apresentadas.

Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 6 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com a área de TI. Deverá ser estabelecido um processo para a renovação de senha (confirmar a

identidade). Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é 45 (quarenta e cinco) dias, não podendo ser repetidas as 3 (três) últimas senhas.

Os sistemas críticos e sensíveis para a logins com privilégios administrativos devem exigir a troca de senhas a cada 30 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, a área de Recursos Humanos deverá imediatamente comunicar tal fato a área de Tecnologia da Informação, a fim de que essa providência seja tomada.

A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares. Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

COMPUTADORES E RECURSOS TECNOLÓGICOS

Todos os equipamentos disponíveis aos colaboradores para acesso à internet são de propriedade do FEU, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A FEU, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem a devida autorização para tal ou credenciamento será

julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor.

DISPOSIÇÕES FINAIS

Ética e segurança devem ser entendidas como parte fundamental da cultura interna da Fundação Editora da Unesp – FEU, sendo que todas as práticas que ameaçam a segurança da informação serão tratadas com a aplicação de ações disciplinares, desde uma advertência verbal até a rescisão contratual por justa causa, levando em consideração os fatores como: função exercida pelo colaborador, período da ocorrência, local, horário e prejuízo real ou potencial causado à Fundação Editora da Unesp – FEU.

.