Política de Segurança da Informação – PSI

Faculdade de Medicina da Universidade de São Paulo - FMUSP

*Dispõe sobre acesso e utilização dos ativos virtuais da **FMUSP**, pelos seus docentes, discentes, servidores/colaboradores e visitantes.*

Os ativos virtuais da **FMUSP** devem ser protegidos contra ações intencionais ou acidentais que impliquem perda, destruição, inserção, cópia, acesso e alteração indevidos, em conformidade com os princípios da **confidencialidade**, **integridade** e **disponibilidade**;

devem ser adotadas medidas de segurança proporcionais aos riscos existentes e à magnitude dos danos potenciais;

as necessidades de segurança devem ser avaliadas com relação a confidencialidade, integridade e disponibilidade;

o acesso aos ambientes lógicos de informações deve ser controlado e estar disponível apenas às pessoas devidamente autorizadas;

os usuários devem ser permanentemente conscientizados sobre os aspectos de segurança e formas de proteção dos recursos e informações sobre sua responsabilidade,

I. DAS CONCEPÇÕES BÁSICAS

Artigo 1º - Para os efeitos desta PSI entende-se por:

1. **ATIVOS VIRTUAIS**: todos os ativos não tangíveis, colocados à disposição dos *usuários*, e que incluem, mas não se restringem as informações necessárias ou não ao desenvolvimento dos trabalhos e a comunicação requerida para transmiti-las, incluindo a telefonia fixa, telefone celular, VOIP,

estação de trabalho, navegação por Internet, E-mails, Instant Messaging, streaming media, e demais serviços e softwares a serem futuramente desenvolvidos pela Instituição ou por terceiros;

USUÁRIO: pessoa física e ou jurídica cadastrada nos ambientes lógicos informatizados, podendo ser docentes, discentes, servidores/colaboradores e outros autorizados envolvidos nas ações da FMUSP, seja no ensino, pesquisa e ou administração, sendo também considerados colaboradores terceiros contratados com anuência do respectivo dirigente, desde de que o Contrato de Prestação de Serviços seja superior a 6 (seis) meses;

HABILITAÇÃO: procedimento que permite ao usuário cadastrado acessar Ambientes lógicos Informatizados;

ACESSO LÓGICO: operação de atualização e consulta de dados e informações em um Sistema.

PERFIL: subconjunto de transações de um Sistema que define a abrangência de atuação do usuário;

TRANSAÇÃO: programa executável do Sistema;

CONFIDENCIALIDADE: princípio de segurança que estabelece restrições ao acesso e a utilização da informação;

INTEGRIDADE: princípio de segurança que trata da confiabilidade da informação;

DISPONIBILIDADE: princípio de segurança que trata da entrega tempestiva da informação a usuários e processos autorizados;

ACESSO IMOTIVADO: aquele realizado para fins estranhos às tarefas do usuário.

II. DO ACESSO AOS ATIVOS VIRTUAIS

Artigo 2º - O acesso do usuário aos ativos virtuais será feito mediante o uso privado de **senha pessoal** e intransferível, sendo que a sua outorga não confere direito de acesso imotivado.

Artigo 3º - O acesso deve ser sempre motivado por **necessidade do desenvolvimento acadêmico e ou administrativo**, com anuência expressa do superior hierárquico em linha direta.

Parágrafo Único – O acesso motivado compreende o conjunto de transações inerentes aos perfis estabelecidos pelo Núcleo de Tecnologia da Informação – **NTI** da **FMUSP**.

Artigo 4º - Caberá ao Núcleo de Tecnologia da Informação **NTI** definir as condições para a adoção, manutenção e controle do acesso aos **ATIVOS VIRTUAIS**, visando, mas não se restringindo a:

1. proteger as informações contra o uso não autorizado;
2. auxiliar na detecção de violações de segurança;
3. assegurar recuperação nas situações de falha;
4. permitir contabilização individual do uso;
5. preservar os dados relativos às transações realizadas, com a identificação do usuário, local, data e horário de acesso.
6. implantar ambientes lógicos 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 ambientes lógicos poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
7. tornar públicas as informações obtidas pelos ambientes lógicos de monitoramento e auditoria, no caso de exigência judicial, solicitação do Diretor da FMUSP;
8. realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

9. instalar ambientes lógicos de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

10. Em relação aos dispositivos moveis a FMUSP, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança. O colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções no âmbito da FMUSP, mesmo depois de terminado o vínculo contratual mantido com a instituição;

Artigo 5º - Os usuários disporão da **SENHA** somente após assinatura do "**TERMO DE RESPONSABILIDADE**", conforme modelo anexo e ou de acordo em documento eletrônico disponibilizados nas aplicações de acesso digital e ou rede sem fio.

III. DAS RESPONSABILIDADES INSTITUCIONAIS E FUNCIONAIS

Artigo 6º – Constituem-se em responsabilidades dos usuários cuidarem da integridade, confidencialidade e disponibilidade dos dados, informações e Ambientes lógicos, devendo comunicar por escrito à chefia imediata **e ou ao NTI** quaisquer irregularidades, desvios ou falhas identificadas.

§1º - O acesso à informação não garante direito sobre a mesma nem confere autoridade para liberar acesso a outras pessoas.

§2º - Os usuários e os cadastradores devem manter suas senhas de acesso secretas, não podendo deixar os ambientes lógicos em condições de ser acessado por terceiros.

Artigo 7º – No tocante aos *servidores/colaboradores* é de responsabilidade da chefia imediata iniciar ação corretiva apropriada para corrigir os desvios com relação às normas desta **PSI** ou procedimentos de segurança dentro de sua área de atuação, comunicando o fato ao Diretor Executivo e ao Coordenador Técnico do **NTI**.

Artigo 8º – O descumprimento das disposições desta **PSI** caracterizará infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo da responsabilidade penal e civil.

Artigo 9º – O acesso imotivado do usuário aos Ativos Virtuais do **FMUSP** constitui, sem prejuízo da responsabilidade civil e penal, infração funcional de falta de zelo e dedicação às atribuições do cargo ou função-atividade e descumprimento de normas legais ou regulamentares.

Artigo 10 – Ressalvadas as hipóteses de requisições legalmente autorizadas, constitui infração funcional a revelação de segredo do qual se apropriou em razão do cargo ou função-atividade, e crime tipificado no Código Penal, a divulgação, a terceiros, de informações dos Ambientes lógicos Informatizados protegidas pelo sigilo, sujeitando o infrator à penalidade de acordo com as normas vigentes.

Artigo 11 – A **FMUSP**, através do Núcleo de Tecnologia da Informação, se reserva o direito de auditar, sempre que julgar necessário, o cumprimento das normas/procedimentos citados nesta **PSI.**

IV. DA UTILIZAÇÃO DO CORREIO ELETRÔNICO (E-MAIL)

SEÇÃO I

Do Acesso

Artigo 12 – Os usuários previstos no artigo 1º, elegíveis terão acesso à utilização do correio eletrônico, mediante o preenchimento da solicitação eletrônica do serviço de e-mail presente no Portal Institucional.

Artigo 13 – O usuário declarará ciência a esta **PSI**, através do aceite eletrônico que deverá ser realizado após a finalização da solicitação do serviço de e-mail.

SEÇÃO II

Das Vedações

Artigo 14 – É vedada a utilização do correio eletrônico nas seguintes hipóteses:

1. envio de mensagens não autorizadas divulgando informações sigilosas e/ou de propriedade da organização;
2. acesso não autorizado à caixa postal de outro usuário:
3. envio, armazenamento e manuseio de material que contrarie o disposto na legislação vigente, a moral e aos bons costumes;
4. envio, armazenamento e manuseio de material que caracterize a divulgação, incentivo ou prática de atos ilícitos, proibidos pela lei ou pela presente Norma, lesivos aos direitos e interesses da organização ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo do usuário ou de terceiros;

5. envio, armazenamento e manuseio de material que caracterize: promoção, divulgação ou incentivo a ameaças, difamação ou assédio a outras pessoas; assuntos de caráter obsceno; prática de qualquer tipo de discriminação relativa a raça, sexo ou credo religioso; distribuição de qualquer material que caracterize violação de direito autoral garantido por lei; uso para atividades com fins comerciais e o uso extensivo para assuntos pessoais ou privados;

6. envio de mensagens do tipo “corrente” e “spam”;

7. envio intencional de mensagens que contenham vírus eletrônico ou qualquer forma de rotinas de programação de computador, prejudiciais ou danosas;

8. envio de mensagens que contenham 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;

9. utilização de listas e/ou catálogo de endereços da **FMUSP** para a distribuição de mensagens que não sejam de estrito interesse funcional e sem a devida permissão da Assessoria de Comunicação;

10. a não disponibilização de aviso de férias e ou licenças/afastamentos superiores a 15 (quinze) dias;

11. ausência de identificação na assinatura do email, composta das seguintes informações: logotipo oficial da **FMUSP**, nome do colaborador, cargo ou função, departamento, telefone(s), localização e endereço eletrônico do site institucional(www.fm.usp.br)

SEÇÃO III

Dos Usuários sem vínculo funcional

Artigo 15 - Para as contas concedidas, em caráter excepcional para terceiros, voluntários, professores associados, ou seja, os que não possuam vínculo empregatício ou acadêmico, a concessão poderá ser dada somente com prazo pré-determinado de no máximo 1 (um) ano, devendo ser renovado, por solicitação da Área Responsável, sendo que se não houver renovação, o acesso será, automaticamente, bloqueado após 10 dias de expiração da concessão.

SEÇÃO IV

Das Boas Práticas

Artigo 16 - Para garantir o uso correto do e-mail corporativo, devem ser observados as seguintes práticas:

1. não use termos coloquiais, mas sim tratamento formal;
2. não utilize a titulação profissional precedendo o nome (Doutor, Professor etc), detendo-se apenas no cargo/função;
3. use o tratamento de senhor (sr.) ou senhora (sra.), e não “você”, independente do cargo, sendo feito uso da primeira pessoa do plural, visto que a comunicação é em nome da Instituição;
4. evite o uso de expressões como “beijos” ao final da mensagem, sendo o correto enviar saudações ou abraços;
5. trate de assuntos gerais de modo discreto e bem-educado evitando-se assuntos muito íntimos, que possam gerar algum tipo de constrangimento;
6. evite o uso de elogios que possam gerar duplo sentido;
7. evite convites a pessoas que sejam subordinados hierárquicos que possam gerar constrangimento e dar a entender eventual assédio moral;

8. evite comentários sobre a Instituição e/ou de pessoas do trabalho, lembrando-se que o ambiente corporativo é monitorado, e como está escrito, não há como alegar que "*não era bem isso o que queria dizer*";

9. não use e-mail e internet corporativa para divulgar currículo;

10. não use ferramentas da Instituição como smartphone ou pen-drive para armazenar conteúdo particular ou fotos mais íntimas;

V. DA UTILIZAÇÃO DA INTERNET/WI FI

SEÇÃO I

Do Acesso

Artigo 17 São elegíveis ao acesso a Internet a partir das dependências da FMUSP. Os usuários. Aos visitantes desde que realizam cadastro de acesso conforme Portal Institucional.

Artigo 18 Os recursos tecnológicos corporativos e serviços fornecidos para o acesso à internet são de propriedade da FMUSP, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, visando assegurar o cumprimento desta PSI.

SEÇÃO II

Das Vedações

Artigo 19 É vedado o acesso a Internet nas seguintes hipóteses**:**

1. download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato);
2. a divulgação e/ou o compartilhamento indevido de informações sigilosas em listas de discussão ou bate-papo;
3. alteração dos parâmetros de segurança, por qualquer colaborador;
4. para uso de software de peer-to-peer (P2P), tais como Kazaa, Emule e afins;
5. Não é permitido acesso a sites de proxy
6. utilizar os recursos de tecnologia da FMUSP para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

SEÇÃO IV

Das Boas Práticas

Artigo 20 - Para garantir o uso correto da Internet/WI-FI no âmbito corporativo, devem ser observadas as seguintes práticas:

1. O usuário deve utilizar a Internet de forma adequada e diligente;

2. O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de sua chave de acesso;

3. não distribuir arquivos do tipo correntes ou manifestos, pois esses causam excessivo tráfego na rede;

4. deve se abster de utilizar a Internet com objetivos ou meio para a prática de atos ilícitos, proibidos pela lei ou pela presente PSI, lesivos aos direitos e interesses do Órgão ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros;

VI. DISPOSIÇÕES FINAIS

Artigo 21 – Cabe ao NTI gerenciar a aplicação das normas desta PSI, expedir atualizações ou instruções complementares, bem como realizar periodicamente auditoria de segurança nos ambientes operacionais e nos ambientes lógicos da FMUSP.

Artigo 22 – Os contratos de prestação de serviços relacionados aos ambientes lógicos informatizados na **FMUSP** devem conter cláusulas que viabilizem a adoção e manutenção das normas de segurança.

Esta **PSI** entra em vigor na data de sua publicação,

São Paulo, 15 de janeiro de 2016

MEDICINA
USP

TERMO DE RESPONSABILIDADE

Declaro que estou ciente das normas contidas na **Política de Segurança da Informação- PSI,** nº ...../....., que "*Dispõe sobre acesso e utilização dos ativos virtuais da* ***FMUSP****, pelos seus docentes, discente, servidores/colaboradores e visitantes"*

Reconheço que a infração a essas normas constitui falta funcional passível de punição nos termos da lei, responsabilizando-me, inclusive, pelos danos que causar a **FMUSP** ou a terceiros, em decorrência da má utilização ou uso indevido que fizer desta autorização para ter acesso aos ativos virtuais da Faculdade de Medicinada Universidade de São Paulo.

São Paulo, de de

_____

Assinatura

Identificação

R.G. Nº