DG DOCUMENTO GERAL	SEGURANÇA EM COMPUTADORES PESSOAIS E PORTÁTEIS

APRESENTAÇÃO

Este documento estabelece normas para a utilização dos recursos de computação pessoal e portátil no ambiente da Sukyo Mahikari do Brasil

DSI DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO	Os comentários e sugestões referentes a este documento devem ser encaminhados ao gestor desse documento indicando o item a ser revisado, a proposta e a justificativa. Este documento normativo tem a validade de um ano a partir da sua edição, prazo máximo para a realização da próxima revisão.

GESTOR: DSI	APROVADOR
Hugo Okamoto	Hidekazu Sakamoto

CONTROLE DE REVISÕES

REV.	DESCRIÇÃO DA MUDANÇA	DATA
0	Emissão original – sem revisões	

SUMÁRIO

1. OBJETIVO

Este documento estabelece normas para a utilização dos recursos de computação pessoal e portátil no ambiente da Sukyo Mahikari do Brasil. Recomenda controles de proteção ao ativo físico, uso adequado, responsabilidade do usuário e prevenção a danos. Este trabalho foi desenvolvido para auxiliar no planejamento e a implementação de mecanismos que garantam integridade e disponibilidade das estações de trabalho.

2. APLICAÇÃO

Esta Política de Segurança da Informação destina-se a todos os funcionários, colaboradores, voluntários e usuários de informações da Sukyo Mahikari do Brasil, servindo de base para a definição de normas específicas, procedimentos, responsabilidades e conceitos.

3. ATRIBUIÇÕES E RESPONSABILIDADES

- Cabe ao DSI, a gestão deste documento que inclui seu desenvolvimento, implementação e manutenção.
- Cabe ao DSI manter este documento atualizado e promover as revisões necessárias.
- Cabe à Diretoria a aprovação deste documento.
- Cabem a todos os funcionários, colaboradores e voluntários a ler e seguir as diretrizes.

4. DOCUMENTOS DE REFERÊNCIA

O presente documento foi desenvolvido com base no seguinte documento externo:

- NBR ISO/IEC 27002, item 10.4.1, 10.4.2

5. TERMINOLOGIA

Malware: O termo malware é proveniente do inglês malicious software; é um software destinado a se infiltrar em um sistema de computador alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informações (confidenciais ou não). Vírus de computador, worms, trojan horses (cavalos de tróia) e spywares são considerados malware.

6. CONCEITO

Este documento referencia os seguintes termos:

a) Computadores Pessoais

São as estações de trabalho, de propriedade da Sukyo Mahikari do Brasil, disponibilizadas para as atividades da organização.

b) Computadores Portáteis

São as estações de trabalho portáteis, de propriedade da Sukyo Mahikari do Brasil ou dos voluntários, utilizadas para as atividades profissionais da Instituição. Enquadram-se nessa categoria:

- Notebooks;
- Assistentes digitais pessoais (PDAs): palmtop, iPaq, pocket PC, aparelhos de telefone celular, smartphones, etc;
- Mídias de leitura e/ou de gravação, como disquetes, CDs, DVDs, memória flash, etc.

c) Acesso aos Recursos

Trata-se da conexão física ou lógica de qualquer equipamento às redes da Sukyo Mahikari do Brasil, efetuada local ou remotamente.

d) Usuário (pessoa física)

Pessoa, funcionário ou não, à qual é dada, explicitamente, a autorização para a utilização de um recurso computacional a fim de executar as atividades relacionadas exclusivamente às atividades da Sukyo Mahikari do Brasil.

7. CONTROLE DE ACESSO À ESTAÇÃO DE TRABALHO

Para o acesso às estações de trabalho e aos computadores portáteis, é necessária a identificação do usuário antes de ter o seu acesso liberado. Seu objetivo é coibir o acesso não autorizado às informações e aos sistemas sensíveis por meio do uso de controles de segurança no que se refere ao sistema operacional.

7.1. Proteção de tela com senha

Todas as estações de trabalho devem estar configuradas para ativar a proteção de tela com senha. Essa proteção deve ser ativada após certo tempo de inatividade da estação de trabalho.

8. SEGURANÇA DA ESTAÇÃO DE TRABALHO

8.1. Uso seguro do equipamento

A integridade e o sigilo das informações armazenadas em estações de trabalho são de responsabilidade do usuário. As normas descritas a seguir destinam-se a todas as estações de trabalho que utilizam os recursos da rede interna da Sukyo Mahikari do Brasil.

- Sua utilização restringe-se exclusivamente aos assuntos das atividades da Sukyo Mahikari do Brasil.
- Deve ser aplicada a configuração da proteção de tela em todas as estações de trabalho, com ativação após certo tempo de inatividade da estação de trabalho.
- Sempre que o funcionário se ausentar do ambiente de trabalho, o acesso ao seu computador deve ser bloqueado, ou o equipamento deverá ser desligado para evitar que sejam utilizados seus recursos de forma ilícita.
- Não devem ser gravadas informações sigilosas ou pertinentes ao trabalho no drive local da máquina. Esse drive não é contemplado pelo processo de backup diário e os dados ali gravados ficam disponíveis a qualquer um que tenha acesso físico à estação de trabalho.
- As informações sensíveis devem sempre ser salvas nos servidores de arquivo da rede interna.
- As salas devem ser trancadas no final do expediente e durante os finais de semana.
- Devem ser utilizados softwares de antivírus e proteção contra malwares em todos os computadores pessoais e nos servidores da Sukyo Mahikari do Brasil. Sua versão deve ser sempre mantida atualizada.
- O acesso de um computador portátil no ambiente computacional da Sukyo Mahikari Brasil só poderá ser concedido mediante solicitação de um dirigente responsável.
- Antes de permitir o acesso ao ambiente computacional da Sukyo Mahikari do Brasil, os computadores portáteis de propriedades dos voluntários devem:
    - Utilizar a rede Wi-Fi da Sukyo Mahikari do Brasil que é isolada e destinada para esse fim ou;
    - Passar por uma avaliação de segurança contendo, no mínimo:
        - Verificação das atualizações de segurança do sistema operacional,

  - Proteção (antivírus) conta malware instalado e atualizado,
  - Realizar uma varredura (scanner) no computador portátil.
- Notebooks deverão sempre ser guardados em local seguro.
- Somente devem ser instalados nos computadores pessoais os softwares fornecidos pela área de tecnologia da informação da Sukyo Mahikari do Brasil, e que tenha o seu uso autorizado. Aqui, incluem-se também os programas e os aplicativos padrões da Instituição.
- Não deve ser copiado ou instalado nenhum software sem o consentimento da Área de Informática.

8.2. Segurança Física

Os equipamentos devem ser instalados e protegidos contra ameaças ambientais, perigos e oportunidades de acessos não autorizados.

Os equipamentos devem ser protegidos contra falhas de energia e outras anomalias na alimentação elétrica. O fornecimento de energia elétrica deve estar em conformidade com as especificações do equipamento.

Os cabeamentos elétricos, de telecomunicações e de dados devem ser protegidos contra interceptação ou dano.

O uso de qualquer equipamento para processamento da informação localizado fora dos limites físicos da organização deve sempre ser autorizado pela administração. A segurança a ser implementada deve ser igual àquela dos equipamentos similares instalados dentro da organização, levando-se em consideração os riscos do ambiente no qual ele está inserido.

8.3. Segurança contra malware

Todos os sistemas computacionais da rede interna devem estar munidos de softwares de verificação contra malware e devem estar regularmente atualizados. Para garantir integridade e proteção das informações, devem ser observadas as seguintes normas:

- Todas as estações de trabalho devem ter um software de antivírus (proteção contra malware) homologado e atualizado pela Instituição;
- É proibida a instalação de qualquer software sem a devida autorização;
- Caso seja detectado algum malware ou suspeite-se da existência de algum, o usuário deve ser instruído a contatar a Área de Segurança da Informação. Em hipótese alguma deverá tentar eliminar o malware por conta própria.