omnisblue

POLÍTICA DE SEGURANÇA EM ESTAÇÕES DE TRABALHO E RECURSOS DE COMPUTAÇÃO MÓVEL

Omnisblue | Departamento de Infraestrutura

1. Histórico de revisão do documento

Abaixo são registrados as versões e atualizações deste documento.

Versão	Data	Autor	Alterações
1.0	03/03/2023	Daniel Zaitz	Versão inicial do documento.

2. Objetivo

Esta política tem como objetivo definir regras de segurança para uso das estações de trabalho (desktops e notebooks) de propriedade da OMNISBLUE, bem como definir os controles necessários para utilização de recursos de computação móvel, como por exemplo, notebooks /laptops, PDAs e celulares.

3. Definições

- Antivírus - Programa ou software especificamente desenvolvido para detectar, anular e eliminar de um computador, vírus e outros tipos de códigos maliciosos.
- Bluetooth - Conexão via Rádio Frequência de curto alcance (em torno de 10m), utilizada para conectar dispositivos, tais como PDAs, celulares, etc;
- Códigos Maliciosos - Código malicioso de computador é um programa – uma parte de um código executável – com capacidade de auto replicação podendo destruir arquivos, formatar a unidade de disco rígido ou causar outros danos.
- Desktop – Computador de mesa;
- Dispositivos de entrada e saída - Os dispositivos de entrada e saída (E/S) ou input/output (I/O) são também denominados periféricos. Eles permitem a interação do processador com o meio externo. Exemplos de dispositivos de entrada de informações são: teclado, mouse e drive de CD / DVD-ROM. Exemplos de dispositivos de saída de informações são: monitor de vídeo, drive de CD-ROM e caixa de som.
- Equipamentos stand alone – Computadores desconectados da rede.
- Notebook / laptop – Computador portátil;
- PDA / Pocket PC - Personal Digital Assistant, é um computador de dimensões reduzidas, com possibilidade de interconexão com computadores pessoais e redes sem fio (wireless). Ex: Palmtop ou Tablet;
- Portas USB (Universal Serial Bus) – Portas utilizadas para conexão de qualquer dispositivo que possua a mesma interface, por exemplo, um "pen drive", dispositivo móvel que permite armazenar até centenas de MBs em dados de qualquer tipo.

- Smartphone - É uma mistura de Telefone Celular com PDA que possui aplicações de gerenciamento de informações pessoais e funções de multimídia;
- Wireless – Mesmo que rede sem fio, permite a conexão entre computadores e outros dispositivos através da transmissão e recepção de sinais de rádio.

4. Controles

- Deve-se estabelecer um processo para identificar vulnerabilidades de segurança recém-descobertas e garantir que todos os componentes de sistema e softwares instalados nas estações de trabalho e recursos de computação móvel possuam a última atualização fornecida pelo fabricante;

5. Uso de equipamentos de computação móvel

- As requisições de equipamentos de computação móvel devem ser direcionadas à Gerência do Solicitante através do formulário Req. Equipamento de Comp Móvel disponível no sharepoint da OMNISBLUE e devem liberadas mediante a comprovação da necessidade do negócio;
- Deve ser mantido um histórico das solicitações de acesso a Recursos de Computação Móvel;
- Não será efetuada cópia de segurança (backup) de informações gravadas em equipamentos de computação móvel;
- É expressamente proibida a conexão de notebooks de propriedade de funcionários, terceiros ou parceiros comerciais à rede da OMNISBLUE a menos que haja aprovação formal da área de Segurança de Informações;
- As requisições de conexão de equipamentos de computação móvel à rede da OMNISBLUE devem ser direcionadas à Gerência do Solicitante através do formulário Termo de acesso remoto – Autorização Comp Móvel disponível na Intranet e devem liberadas mediante a comprovação da necessidade do negócio;
- A troca/sincronismo de dados entre recursos de computação móvel e computadores da OMNISBLUE, ligados à rede ou não, é proibida a menos que o recurso seja de propriedade da OMNISBLUE e devidamente identificado com número de patrimônio;
- Não é permitida a armazenagem de dados de Portadores de Cartão em equipamentos de computação móvel.

6. Proteção dos equipamentos

- O usuário de recursos de computação móvel de propriedade da OMNISBLUE é responsável por proteger fisicamente o equipamento que está utilizando contra roubo e furto;
- O usuário deve notificar imediatamente a sua gerência e a área de TI – Segurança da Informação, caso seu equipamento móvel seja perdido ou quando suspeitar que ele possa ter sido comprometido de alguma maneira;
- O usuário deve observar a qualquer tempo as instruções do fabricante para proteção do equipamento, por exemplo, proteção contra exposição a campos eletromagnéticos intensos;
- Os equipamentos não devem, em hipótese alguma, ser deixados sem supervisão fora das dependências da empresa. Ex: Aeroportos, aviões e outros meios de transporte, quartos de hotéis, centros de conferência, locais de reunião ou porta-malas de veículos;
- Os equipamentos devem ser carregados como bagagem de mão e disfarçados, sempre que possível, quando se viaja;
- Equipamentos que contém informações importantes, sensíveis e/ou críticas para o negócio devem ser fisicamente trancados ou protegidos com travas especiais sempre que for necessário deixá-los sem supervisão.