Política de Segurança Institucional da Rede CBIOT

1 Regras Gerais:

O uso dos computadores conectados à rede do Centro de Biotecnologia da UFRGS (CBIOT), independentemente de pertencerem à Universidade ou serem de propriedade privada, deve estar em conformidade com a Política de Rede do CBiot, de acordo com as Regras da Universidade:

1.1 As credenciais de acesso à rede (login e senha) são de uso individual e não podem ser compartilhados com terceiros, sob pena de suspensão ou cancelamento das credenciais.

1.2 A guarda das informações de login e senha de acesso são de total responsabilidade de cada usuário, bem como todas as atividades e acessos efetuados através dessa conta.

1.3 É obrigatório o uso de um bom antivírus nos computadores conectados à rede, devendo o mesmo estar sempre atualizado.

1.4 Os usuários deverão respeitar os direitos autorais, licenças de software e de outros recursos disponíveis ou enviados através da rede (músicas, vídeos, textos, imagens, etc).

1.5 A Administração do CBiot poderá solicitar ao Supervisor de Rede relatórios de conexões e acessos realizados na rede CBiot, apontando usuários e/ou logins, sempre que necessário ou para fins de estatística

1.6 O suporte em Tecnologia da Informação (TI) do CBIOT não é responsável por máquinas que não possuem patrimônio da Universidade. Máquinas ou equipamentos particulares ficam sob total responsabilidade do proprietário ou portador.

1.7 Máquinas ou equipamentos particulares devem passar por avaliação do Suporte de TI antes de ser conectado à rede do CBIOT. O proprietário ou portador da máquina deverá fornecer acesso de administração à máquina/equipamento para que sejam instalados softwares necessários para esta avaliação.

1.8 Quaisquer problemas ou suspeita de problemas relacionados a **questões de segurança da informação**, **deverão ser informados, via e-mail, para suporte@cbiot.ufrgs.br, ou para a Administração do CBIOT**.

2. É proibido:

2.1 Acessar computadores, softwares, dados, informações ou outros recursos de informação, em redes locais ou externas, sem a devida autorização ou, intencionalmente, habilitar outros a fazerem isso.

2.2 Utilizar programas e recursos que causem ou tentem causar a indisponibilidade de serviços de rede ou que prejudiquem de alguma forma as atividades de outros usuários.

2.3 Efetuar ações que possam ser caracterizadas como violação da segurança computacional (utilização de sniffers, efetuar probes ou varreduras na rede, quebrar a senha de outras contas, etc).

2.4 Utilizar recursos de comunicação (como e-mail, instant messengers ou sistemas com funções similares) para o envio de mensagens fraudulentas, hostis, obscenas, ameaçadoras, antiéticas ou outras mensagens que violem as leis federais, estaduais ou outras leis ou políticas da Universidade.

2.5 Utilizar programas de compartilhamento de arquivos do tipo peer-to-peer (p2p), tais como kazaa, eMule, LimeWire, BitTorrent, etc. O objetivo desta proibição é prevenir a pirataria e assegurar o uso adequado dos recursos da rede.

2.6 Qualquer violação de direitos autorais, downloads de arquivos infectados ou maliciosos, e abuso no uso da rede (grande volume de downloads de músicas, vídeos, programas, etc) acarretará em advertência, seguida de suspensão de conexão com a internet, podendo ser aplicadas as penalidades constante no item 2.11.

2.7 Não é permitida a instalação de qualquer programa adquirido com recursos próprios nas máquinas que fazem parte do patrimônio da Universidade, sem prévia consulta ao Suporte de TI.

2.8 Alterações nas configurações de rede (IP, DNS, WINS, máscara de rede, ROUTER, etc) das máquinas conectadas a rede do CBiot não devem ser alteradas sem o conhecimento do Suporte de TI e posterior autorização da Administração do CBiot. As configurações de rede são entregues via DHCP e devem permanecer como entregues.

2.9 É vetada a utilização de servidor proxy ou ferramentas que permitem este tipo de conexão (UltraSurf e afins).

2.10 O acesso excessivo às Redes Sociais (Facebook, twitter, etc) ocasionará no bloqueio daquele usuário a tais conexões. Salientamos que o Suporte de TI tem permissão para monitorar a utilização usuário/frequência, e quando constatado o uso abusivo, mediante avaliação do Líder de Grupo e da Direção, será realizado o bloqueio.

2.11 O não seguimento das políticas definidas acima poderão implicar em perda de conexão à rede do CBIOT. Se o incidente configurar ilícito penal ou administrativo, as instâncias cabíveis da Universidade serão acionadas.

A conexão com a rede do CBIOT implica na aceitação de TODOS os termos citados neste documento.