Anexo I
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. A presente política é definida pelo conjunto de regras gerais que direcionam a segurança da informação e são suportadas por normas e procedimentos que deverão ser seguidos por toda a organização.

2. Estabelece procedimentos para utilização correta dos ativos de tecnologia da informação, a fim de evitar incidentes que possam: inutilizar, extinguir ou alterar dados.
Promover ainda, a conscientização para com a segurança da informação e meios que contribuam para a manutenção dos princípios da segurança da Informação e seus aspectos:
Confidencialidade, Integridade e Disponibilidade, Autenticidade e Não repúdio.

3. Política de Uso da Internet:

a) O colaborador não deverá compartilhar sua credencial de acesso ao computador a terceiros, caso contrário se responsabilizará pelo acesso indevido;
b) É vedado o acesso a sites que estejam fora do interesse da empresa, como: bate papo, redes sociais, conteúdo ofensivo, racista ou pornográfico, a empresa poderá definir exceções;
c) É vedado o acesso a sites de estrutura duvidosa que ofereçam risco à segurança da informação ou que possuam ferramentas que visem burlar os mecanismos de segurança da empresa ou ocultar as credenciais de acesso à internet, como navegadores anônimos e proxy anônimo;
d) A critério da empresa, sites com conteúdo não pertinente ao trabalho, terão o acesso bloqueado;
e) O colaborador que fizer mau uso da internet, terá o acesso bloqueado.

4. Uso da rede Sem Fio: a empresa disponibiliza a rede sem fio (Wi-Fi) Corporativa e outra para acesso de Visitantes. O colaborador deverá utilizar com os mesmos princípios do item supra.

5. Uso da Rede Cabeada: a utilização da rede cabeada deverá ser realizada por dispositivos autorizados, terão seu acesso à Internet permitido de acordo com o grupo de liberação, para que funcionem de acordo com a política de segurança da Informação.

6. Política de Acesso aos Arquivos da Rede: todos os arquivos deverão ser salvos na rede, nas pastas dos respectivos departamentos, onde serão realizados *backups* periódicos. **Fica vedado** salvar arquivos no disco do computador pessoal de trabalho, pen drive, HD externos ou outro meio.

7. Política de Uso do E-mail:

a) O e-mail deverá ser utilizado apenas para os interesses da empresa, não devendo ser utilizado para fins particulares, envio de spams, propaganda, conteúdo impróprio, difamatório, calunioso ou que prejudique a imagem da empresa e seus colaboradores;
b) O colaborador deverá utilizar senha com a complexidade descrita nesta política de segurança e não fornecer sua senha para terceiros sob nenhuma hipótese;
c) O acesso do email deverá ser realizado através da plataforma que a empresa indicar;

d) O colaborador não deverá abrir e-mails de origem duvidosa, ou que julgar não pertinentes ao trabalho, incluindo anexos. Diante de qualquer dúvida deverá entrar em contato com o área de TI e mover a mensagem suspeita para a caixa de spam;
e) A camada de segurança AntiSpam poderá classificar o email como provável spam ou bloquear a mensagem, caso seja classificado como spam.

8. Política de Uso dos Computadores:

a) O acesso aos computadores, sistemas e arquivos da rede da empresa será fornecido através de credenciais de acesso de uso pessoal, a credencial de acesso será composta por login e senha;
b) A senha deverá ser composta de no mínimo 4 caracteres, podendo ser alfabética e/ou numérica;
c) A senha de acesso aos computadores
será alterada a cada 180 (cento e oitenta) dias;
d) Todo computador deverá possuir sistema antivírus instalado,
ativo e atualizado que será fornecido, instalado e monitorado pela equipe de TI;
e) Não deverão ser instalados softwares não homologados pelo administração, softwares piratas, softwares para fins que não são do interesse da empresa ou não relacionados com a função do colaborador;
f) Somente os administradores estão autorizados à instalar softwares de qualquer natureza;
g) Não deverão ser baixados e/ou executados arquivos desconhecidos ou fora do interesse da empresa, que possuam as extensões: .exe, .com, .bat,.pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf, ou qualquer outra extensão que represente um risco à segurança;
h) Os computadores poderão ser monitorados e auditados pelos administradores a qualquer tempo, para fim de verificação de conformidade com a política de segurança da informação;
i) Os computadores terão programas de cadastramento padronizados: utilizando as mesmas impressoras e unidades de rede mapeadas;
j) O colaborador deverá bloquear seu computador quando ausentar-se do departamento,mesmo que por breve período de tempo, se o tiver que se ausentar por tempo indeterminado deverá desligar o computador;
k) Não será fornecida credencial de acesso do tipo Administrador.

9. Política de Senha e Acesso:

a) A senha de acesso de um novo colaborador de qualquer sistema deverá ser requisitada diretamente para o administrador por meio de e-mail no endereço gavitti@bol.com.br fornecendo dados básicos para preenchimento de formulário de solicitação de acessos,
b) A senha de acesso aos sistemas e computadores é de uso pessoal e não deve ser compartilhada;
c) A senha de acesso deve ser composta por no mínimo 04 dígitos,podendo ser alfabética e/ou numérica;
d) Após 3 (três) tentativas seguidas de acesso com senha inválida, a senha será bloqueada e o colaborador deverá entrar em contato com o administrador por meio de e-mail no endereço gavitti@bol.com.br para desbloqueio da senha;
e) As senhas terão validade de 180 (cento e oitenta) dias, após esse período deverão ser alteradas para uma nova senha.

10. Auditoria e Registros de Logs:

a) Credenciais de Acesso, serão registrados em logs automáticos, todos os acessos dos usuários aos recursos da empresa, incluindo acesso aos sistemas, criação, exclusão e alteração de arquivos, horário de logon na máquina, utilização de impressora e outros sistemas.

b) Arquivos Pessoais, não será permitido a guarda de arquivos pessoais na rede da empresa, que incluem: músicas, imagens, vídeos e outros arquivos em geral.

11. Política de Uso de Dispositivos Pessoais (Celulares, Tablets, Notebook):
será permitido o uso de dispositivos pessoais, como notebook, desde que estejam de acordo com as políticas de segurança da informação da empresa.

12. Política de Uso de Impressoras: a quantidade de impressões, será registrada em Log, e poderá ser auditada quanto ao colaborador que imprimiu, quantidade de páginas, nome do arquivo impresso. O uso das impressoras deverá ser feito para os interesses da empresa e utilizadas com consciência ecológica.

13. Política de *Backup* e Contingência:
a) Procedimento de Backup dos Arquivos e Bancos de Dados, o *backup* será realizado maneira automatizada obedecendo as diretrizes do software MERCABOM (lupasoft).

14. Política de Controle de Acesso à Infraestrutura:

a) Bloqueio de Acesso a funcionários Desligados/afastados; os funcionários desligados ou afastados por período superior a 07 (sete) dias terão suas credenciais de acesso aos sistemas, computadores, e-mail e ambiente de rede, sejam bloqueadas;

b) Registro de Chamados diante de qualquer incidente ou pedido de suporte, deverá ser registrado o pedido ou a demanda através de sistema indicado pela empresa ou através de email. gavitti@bol.com.br

15. Responsabilidades:
a) ADMINISTRADORES: manter e atualizar essa política de segurança da Informação periodicamente, bem como apoiar a implementação da presente política.
b) Colaboradores, cumprir as políticas de segurança da informação e contribuir para sua melhoria e eficiência.

16. Cumprimento: diante do descumprimento desta política em geral, o colaborador poderá, a qualquer tempo, ser auditado, através da equipe de TI e poderá receber em consequência, a aplicação de ações disciplinares cabíveis que se fizerem necessárias.