CARTILHA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO
GUIA DA BOAS PRÁTICAS

1. Segurança da Informação

A LUFT preza pelo uso seguro e consciente dos recursos tecnológicos e informações da empresa, e por isso desenvolveu um guia de boas práticas, o qual recomenda que todos sigam, garantindo assim não somente a proteção da empresa, mas a proteção de todos os funcionários contra as ameaças cibernéticas que estão em constante evolução.

Lembre-se, a segurança da informação é responsabilidade de TODOS. Contamos com você!

2. Usuários e senhas

O seu usuário e senha representa quem você é no mundo digital, por isto, é essencial que você entenda que eles são intransferíveis, e não poderão ser emprestados em nenhuma condição.

Para garantir a sua proteção, utilize as dicas a seguir:

- Não anote ou armazene sua senha em locais sem proteção, que são visíveis para terceiros;
- Quanto maior melhor. Uma boa senha é grande, use uma frase que seja simples de lembrar para você;
- Não utilize a mesma senha em sistemas diferentes;
- Nunca utilize credenciais emprestadas para acessos aos sistemas corporativos.

3. Acesso corporativo à Internet

O acesso à Internet é concedido de acordo com as suas funções de trabalho, e deve ser usado com responsabilidade. A Internet é a fonte da maioria das ameaças à a sua segurança, sendo assim, recomendamos que:

- Utilize a Internet primariamente para atividades de trabalho;
- Não acesse sites com conteúdo suspeito;
- Não abra links provenientes de e-mails com o remetente desconhecido;
- Durante o acesso à Internet, caso seja solicitado a instalação de algum programa terceiro, entre em contato com a equipe de TI;
- Caso o seu computador tenha algum comportamento estranho durante o acesso à Internet, entre em contato com a equipe de TI.

Lembre-se que para sua segurança, todos os acessos a Internet são monitorados.

4. Redes Sociais

A LUFT não autoriza seus funcionários a compartilhar fotos ou vídeos do ambiente de trabalho e de outros funcionários, a menos que seja concedida uma autorização formal.

5. E-mail e softwares de troca de mensagens instantânea

Fornecemos para nossos funcionários o serviço de e-mail e troca de mensagens instantânea. Use-os apenas para enviar e receber mensagens relacionadas a assuntos de trabalho ou do interesse da empresa. Lembre-se que ao utilizar estas ferramentas você representa a empresa.

Recomendações para garantir a sua segurança e a segurança da empresa:

- Não abra mensagens ou conteúdos como links e arquivos anexos de remetentes desconhecidos;
- Não participe de correntes de mensagens;
- Evite o envio de mensagens para pessoas desnecessárias;
- Antes do envio de uma mensagem, pense se o conteúdo poderá prejudicar a empresa, e avalie se o destinatário deve mesmo receber esta mensagem.

Lembre-se que para sua segurança, todos os e-mails são monitorados.

6. Uso de computadores e recursos tecnológicos

Fornecemos um computador e ou recursos tecnológicos para que os funcionários realizem as suas funções de trabalho. Todas as informações geradas nos computadores e recursos tecnológicos pertencem a LUFT.

Recomendações para garantir a sua segurança e a segurança da empresa:

- Não altere as configurações dos recursos fornecidos sem a autorização da equipe de TI;
- Não instale nenhum programa terceiro sem autorização da equipe de TI;
- Se precisar abrir arquivos de um pendrive, utilize o antivírus para verificar se o pendrive contém algum arquivo malicioso. Se não souber como fazer isso, entre em contato com o time de TI.

7. Mesa limpa e ambiente protegido

Mantenha o ambiente da empresa seguro começando pela sua mesa. Ao se ausentar de sua mesa, garanta que:

- Documentos confidenciais, ou que considere importantes estão protegidos, preferencialmente em armários com chaves;
- Que seu computador está bloqueado;
- Que dispositivos móveis como notebooks, pendrives, tablets e smartphones estejam seguros e protegidos e não fiquem expostos na mesa;
- Se imprimir algo, usa a funcionalidade de senha para que a impressão seja liberada somente quando digitar a senha na impressora. Caso perceba que existem documentos confidenciais que não pertencem a você na impressora, entre em contato com a equipe de TI.

8. Terceiros

Com relação a terceiros, devemos tomar algumas precauções importantes:

Nunca envie informações críticas e confidenciais para terceiros sem antes possuir um acordo de confidencialidade (NDA);

- Terceiros deverão sempre estar acompanhados por um funcionário durante o acesso as dependências da empresa;
- As credenciais de acesso serão fornecidas para terceiros somente depois do NDA e política de segurança estarem assinados.
- Os terceiros devem cumprir as mesmas regras de segurança que os funcionários.

9. Incidentes de segurança

A LUFT possui uma equipe de profissionais experientes para solucionar qualquer tipo de incidente de segurança.

Caso perceba:

- Comportamentos estranhos de seu computador ou de qualquer recurso tecnológico;
- Comportamentos suspeitos de terceiros ou funcionários;
- Políticas e normas de segurança não sendo seguidas;

Acesse a ferramenta do ServiceDesk e abra um chamado de incidente de segurança.

10. Responsabilidades

Lembre-se que você é responsável por todas as suas ações.

Caso existam infrações relacionadas a política e normas de segurança cibernética e da informação serão atribuídas penalizações de acordo com o impacto destas infrações para a empresa. Estas penalizações podem variar de advertências a demissão por justa causa.

Lembre-se das regras de ouro:

- A segurança é de responsabilidade de todos, e TODOS os funcionários independente da posição devem conhecer e cumprir fielmente a política e normas de segurança da informação;
- Incidentes de segurança devem ser comunicados no momento da ocorrência através da ferramenta de ServiceDesk;
- Proteja a informação. Sempre que precisar compartilhar algo com terceiros, avalie se o mesmo precisa ter acesso a esta informação.

Em caso de dúvidas, consulte a POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO em conjunto de suas respectivas NORMAS na INTRANET.