Empresa de roupa que trabalha de forma online

1 Políticas de Uso e Acesso à Rede/Arquivos da Empresa.

1- Garantir que informações sensíveis, como dados de clientes, transações financeiras, e registros internos, sejam acessadas apenas por funcionários autorizados.

2- O acesso a dados sensíveis deve ser restrito de acordo com o cargo e a necessidade de cada colaborador.

3- Uso de autenticação de múltiplos fatores, para acessos a sistemas e arquivos confidenciais.

4- Registros de acesso e alterações devem ser mantidos e monitorados para auditoria e segurança.

2 Política de Uso de Dispositivos e Redes

1 -Estabelecer diretrizes sobre o uso de dispositivos, como computadores, celulares, etc, e redes corporativas.

2- Apenas dispositivos fornecidos ou autorizados pela empresa podem ser usados para acessar os sistemas da empresa.

3- Exigir conexões seguras para acesso remoto à rede corporativa, como VPNs ou conexões criptografadas, para proteger dados durante o tráfego.

4- O uso de dispositivos ou redes da empresa para fins pessoais.

3 Política de Uso de Senhas

1- Definir diretrizes para a criação e gerenciamento de senhas seguras.

2- As senhas devem ter pelo menos 8 caracteres e incluir uma combinação de letras maiúsculas, minúsculas, números e caracteres especiais.

3- Senhas devem ser alteradas regularmente, por exemplo, a cada 90 dias.

4- Proibir o uso de senhas óbvias, como "123456" ou "senha".

4 Política de Acesso e Compartilhamento de Arquivos Externos

1- Definir como os arquivos podem ser compartilhados com partes externas à empresa (clientes, fornecedores, parceiros).

2- Sempre que possível, utilizar plataformas seguras para o compartilhamento de arquivos ,por exemplo, Google Drive ou Dropbox corporativo.

3- Arquivos sensíveis compartilhados com partes externas devem ser criptografados, tanto em repouso quanto em trânsito.

4- O compartilhamento de arquivos com partes externas deve ser autorizado e monitorado para evitar vazamento de informações.

5 Política de Uso de E-mail Corporativo

1- Estabelecer regras para o uso adequado do e-mail corporativo.

2- O e-mail corporativo deve ser utilizado exclusivamente para fins profissionais.

3- Proibir o recebimento e envio de anexos de fontes não confiáveis, para evitar riscos de malware.

4- Os colaboradores devem ser treinados para identificar e-mails fraudulentos (phishing) e tomar as ações apropriadas.

6 Política de acesso temporário

1- Garantir que acessos temporários a sistemas ou arquivos sejam concedidos de forma segura e controlada.

2- O acesso temporário deve ser concedido apenas quando necessário (exemplo: consultores, contratados externos), e sempre por um período limitado.

3- Todo acesso temporário deve ser monitorado e registrado para auditoria.

4- Após o término da necessidade de acesso, o acesso deve ser revogado imediatamente para evitar riscos.

7 Política de Controle de Dispositivos Móveis

1 -Estabelecer regras para o uso de dispositivos móveis, como smartphones e tablets, dentro do ambiente corporativo.

2- Colaboradores podem usar seus próprios dispositivos móveis, mas devem seguir as diretrizes de segurança da empresa (como instalação de software antivírus e criptografia de dados).

3- Implementar soluções de Mobile Device Management (MDM) para controlar e proteger dispositivos móveis corporativos.

4- Em caso de perda ou roubo de um dispositivo, os dados corporativos devem ser remotamente apagados para proteger informações sensíveis.

8 **Política de Manutenção de Hardware**

1- Garantir a manutenção adequada dos equipamentos de TI da empresa para garantir o funcionamento adequado e a segurança.

2- Todos os dispositivos de hardware, como servidores, computadores e roteadores, devem passar por manutenção preventiva e atualizações regulares.

3- Reparos ou modificações em equipamentos devem ser feitos apenas por técnicos autorizados e credenciados pela empresa.

4- Todos os serviços de manutenção devem ser registrados para garantir o rastreamento de alterações e reparos.

9 **Política de Uso de Software Licenciado**

1- Garantir que a empresa utilize apenas software licenciado e evite riscos legais relacionados ao uso de pirataria de software.

2- A empresa deve manter um inventário atualizado de todos os softwares licenciados que estão em uso, garantindo que cada software tenha a licença apropriada.

3- Nenhum colaborador pode instalar software não licenciado ou não autorizado nos sistemas da empresa sem prévia aprovação.

4-Realizar auditorias periódicas para garantir que todos os softwares utilizados na empresa estejam em conformidade com as licenças adquiridas.

10 Política de Compartilhamento de Senhas

1- Proibir o compartilhamento de senhas e garantir que os colaboradores sigam boas práticas de segurança.

2- O compartilhamento de senhas entre colaboradores não é permitido, mesmo que entre equipes ou superiores hierárquicos.

3- Quando for necessário compartilhar credenciais (em casos excepcionais), deve ser utilizado um gerenciador de senhas corporativo aprovado pela empresa.

4 -Cada colaborador deve manter suas senhas pessoais de acesso e garantir que não sejam divulgadas.

11 Política de Uso de Impressoras e Dispositivos de Cópia

1- Estabelecer diretrizes para o uso de impressoras e dispositivos de cópia de forma segura e eficiente.

2- Documentos sensíveis não devem ser impressos em dispositivos compartilhados, a menos que sejam acompanhados e retirados imediatamente após a impressão.

3- Limitar o número de impressões e cópias para reduzir o desperdício e proteger informações confidenciais.

4- Implementar sistemas de monitoramento para rastrear quem e quando fez impressões de documentos sensíveis.

12 Política de Comunicação e Colaboração Online

1- Garantir que as plataformas de comunicação online (e-mail, chat, videoconferência) sejam usadas de maneira profissional e segura.

2- As ferramentas de comunicação online devem ser usadas apenas para fins profissionais e relacionados ao trabalho.

3- Informações sensíveis não devem ser discutidas por canais de comunicação não criptografados (ex: e-mails não seguros).

4 - Garantir que as plataformas de videoconferência e ferramentas de chat estejam em conformidade com as políticas de segurança de dados da empresa.

13 Política de Atualização de Sistemas

1- Garantir que todos os sistemas e softwares da empresa sejam mantidos atualizados com os patches de segurança mais recentes.

2- Os sistemas operacionais, software corporativo e antivírus devem ser atualizados regularmente para corrigir vulnerabilidades de segurança.

3- Sempre que possível, as atualizações de segurança devem ser configuradas para serem feitas automaticamente, sem a necessidade de intervenção manual.

4- Após atualizações críticas, realizar testes para garantir que os sistemas continuem funcionando conforme esperado.

14 Política de Gestão de Incidentes de Segurança

1- Estabelecer um processo claro para a resposta e resolução de incidentes de segurança cibernética.

2- Qualquer colaborador que detectar uma possível violação de segurança (como phishing, acesso não autorizado, etc.) deve reportar imediatamente ao departamento de TI ou segurança.

3- A empresa deve ter um plano de resposta a incidentes documentado, incluindo procedimentos claros sobre como lidar com vazamentos de dados, ataques de malware, e outros tipos de violação.

4- Realizar treinamentos regulares com todos os colaboradores sobre como identificar e agir diante de incidentes de segurança.

15 Política de Monitoramento de Rede

1-Garantir a segurança da rede da empresa por meio do monitoramento contínuo de tráfego e acessos.

2-A empresa deve utilizar ferramentas de monitoramento de rede para detectar comportamentos anormais, acessos não autorizados e atividades suspeitas.

3-Quando uma ameaça é detectada, deve haver um sistema de notificação imediata para as equipes de segurança para que possam tomar medidas corretivas.

4-O monitoramento deve ser feito de maneira ética, respeitando a privacidade dos colaboradores, e sendo realizado apenas em conformidade com a legislação vigente.

16 Política de Uso de Comunicação Externa (e-mail e telefone)

1-Definir diretrizes claras sobre o uso de e-mail e telefone para comunicações externas.

2-O e-mail corporativo deve ser utilizado exclusivamente para atividades relacionadas ao trabalho. E-mails pessoais não devem ser enviados ou recebidos durante o expediente.

3-O uso de telefones corporativos deve ser restrito a chamadas relacionadas ao trabalho. Chamadas pessoais devem ser minimizadas, especialmente em horas de pico.

4-É proibido compartilhar informações confidenciais da empresa por telefone ou e-mail sem a devida autorização e encriptação quando necessário.

17 Política de Descarte de Dados

1-Estabelecer regras para o descarte seguro de dados que não sejam mais necessários para a operação da empresa.

2-Todos os dados sensíveis ou confidenciais devem ser destruídos de forma segura (ex: usando softwares de destruição de dados ou dispositivos físicos) quando não forem mais necessários.

3-Equipamentos obsoletos ou danificados, como computadores, HDs ou servidores, devem ser descartados de maneira segura, garantindo a exclusão total dos dados armazenados neles.

4-O processo de descarte de dados deve ser documentado para garantir rastreabilidade e conformidade com as normas de proteção de dados.

18 Política de Treinamento e Conscientização em Segurança

1- Garantir que todos os colaboradores estejam bem informados sobre as melhores práticas de segurança cibernética e proteção de dados.

2- Todos os funcionários devem receber treinamentos periódicos sobre segurança da informação, proteção de dados pessoais e boas práticas de segurança cibernética.

3- Realizar simulações de phishing e outros tipos de ataques cibernéticos para treinar os colaboradores a identificar e reagir de forma apropriada a ameaças.

4- A empresa deve manter todos os colaboradores informados sobre novas ameaças e mudanças nas políticas de segurança da empresa.

19 Política de Uso de Sistemas de E-commerce

1- Estabelecer regras para o uso dos sistemas de e-commerce da empresa, incluindo a plataforma de vendas online.

2- O acesso ao painel de administração do site de e-commerce deve ser restrito a funcionários autorizados, com autenticação forte (ex: autenticação de dois fatores).

3- Todas as transações financeiras (como pagamentos e informações de cartão de crédito) devem ser processadas por sistemas seguros e em conformidade com as normas de segurança de pagamentos (PCI-DSS).

4- As atualizações de segurança do sistema de e-commerce devem ser feitas regularmente para corrigir vulnerabilidades e melhorar a proteção contra fraudes.

20 Política de Uso de Software de Colaboração (Chat, Videoconferência, etc.)

1- Definir como os colaboradores devem usar ferramentas de colaboração online, como chats corporativos e videoconferências, para garantir a segurança e a conformidade.

2- Ferramentas de colaboração devem ser usadas para fins profissionais. O uso para fins pessoais deve ser restrito durante o horário de expediente.

3- Reuniões virtuais que contenham informações confidenciais devem ser protegidas com senhas, e os links de acesso devem ser enviados apenas aos participantes autorizados.

4- Mensagens e arquivos compartilhados em ferramentas de colaboração devem ser armazenados de forma segura e acessíveis apenas a colaboradores autorizados.