Revisão:	Data de Elaboração:	Data de publicação:	Data de revisão:
01	27/05/2021	30/06/2021	30/06/2022

Unidade Responsável:	Aprovada por: _____
Comitê do Sistema de Integridade da H&P	Diretoria da H&P

SÚMÁRIO

1. OBJETIVO

A presente Política de Segurança da Informação ("Política" ou "PSI") tem como objetivo estabelecer diretrizes estratégicas de segurança da informação para a Herkenhoff & Prates ("H&P"), preservando seus ativos de informação, assim como a sua imagem institucional. As diretrizes propostas visam garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações, bem como atitudes adequadas para manuseio, tratamento, controle e proteção dos dados, informações, documentos e conhecimentos produzidos, armazenados, sob guarda ou transmitidos por qualquer meio ou recurso da H&P contra ameaças e vulnerabilidades. Esta Política também se propõe a orientar os colaboradores da H&P e aqueles que com ela se relacione a H&P no que diz respeito à gestão de riscos e ao tratamento de incidentes de Segurança da Informação, em conformidade com as disposições constitucionais, legais e regimentais vigentes. A PSI estabelece o comprometimento da alta direção organizacional da empresa, com vistas a prover apoio para a implantação do Programa de Privacidade da H&P.

2. APLICAÇÃO

As regras contidas nesta Política devem ser respeitadas pelos sócios, comitês de assessoramento, diretores executivos, colaboradores próprios ou não, estagiários, menores aprendizes, prestadores de serviço e por qualquer pessoa que atue em nome da H&P ou que com ela se relacione.

3. AMBIENTE NORMATIVO

Esta Política foi elaborada em consonância com todas as leis e regulamentações aplicáveis, incluindo, mas sem limitação: Código de Conduta da H&P; Lei Geral de Proteção de Dados (LGPD) nº 13.709/2018; ABNT NBR ISO/IEC 27001:2013; ABNT NBR ISO/IEC 27002:2013; ABNT NBR ISO/IEC 27006:2015.

4. DIRETRIZES GERAIS

- Esta Política contém as diretrizes gerais do sistema de gestão de segurança da informação praticado pela H&P e é a base para as demais políticas específicas para os temas de segurança da informação;
- Os principais conceitos, termos e definições utilizados no decorrer desta PSI se encontram no Anexo I – Glossário;
- Todos os usuários da rede corporativa, sistemas de informação e hardware de TI da H&P devem ser orientados em relação ao uso das informações e dos recursos de Tecnologia da Informação, portanto, devem estar cientes sobre as regras contidas nos documentos que compõem o Código de Conduta da H&P e esta Política de Segurança da Informação;
- As informações da H&P são consideradas patrimônio e devem ser protegidas adequadamente;
- Mecanismos de proteção devem ser adotados para garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações durante todo o seu ciclo de vida;
- O acesso às informações deve ser controlado e limitado às necessidades profissionais de cada usuário;
- Incidentes de Segurança da Informação devem ser notificados à área de Tecnologia da Informação ("TI") da H&P;
- Um modelo de Governança de TI e Segurança da Informação específico da H&P deve ser estabelecido, implementado e mantido de forma que as estratégias sejam definidas, coordenadas, monitoradas e alinhadas ao planejamento estratégico da empresa, com mecanismos de contingência identificados, definidos, implementados e mantidos para os processos de negócios considerados críticos;
- Devem ser firmados previamente contratos com termos de confidencialidade e de proteção à propriedade intelectual e de dados e informações, para fornecedores (parceiros ou terceiros) para implementação e manutenção de sistemas de informação da H&P;
- Sempre que for necessário envolver algum colaborador para a implementação e manutenção de sistemas de informação, as soluções produzidas devem preservar todos os direitos de propriedade

intelectual e resguardar os dados e informações para a H&P, conforme Código de Conduta e termo de confidencialidade, dos quais todos os colaboradores são signatários.

5. RESPONSABILIDADES

5.1 Colaboradores

- Cumprir fielmente esta Política, as Normas e os Procedimentos de Segurança da Informação da H&P;
- Assinar e praticar o Termo de Compromisso, Sigilo e Confidencialidade e demais documentos referentes a guarda e uso de equipamentos da H&P;
- Proteger as informações contra acesso, divulgação, modificação ou destruição não autorizados pela H&P;
- Garantir os cuidados mínimos com a segurança da informação, quando as atividades executadas forem fora dos escritórios da H&P, como no caso de home office, reuniões externas, clientes ou viagens;
- Garantir que equipamentos e recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela H&P;
- Zelar pela rede, pelos equipamentos e recursos tecnológicos que utiliza, não sendo permitido qualquer remoção, desconexão de partes, substituição, reconfiguração ou qualquer alteração nas características físicas ou técnicas dos equipamentos integrantes da rede;
- Realizar de acordo com os procedimentos internos o armazenamento de arquivos de trabalho, respeitando a classificação da informação, a lógica de utilização das nuvens corporativas coletiva e individual (respectivamente, SharePoint e OneDrive for Business), bem como a organização de pastas estabelecidas no SharePoint;
- Comunicar ao coordenador a necessidade de sincronizar pastas do ambiente corporativo de arquivos (SharePoint) para equipamentos, especificando sua finalidade;
- Respeitar os procedimentos internos de compartilhamento de arquivos de trabalho;
- Observar os procedimentos de backup de acordo com disposto nesta Política e em outras normas e orientações da área de TI;

- Descartar adequadamente os documentos de acordo com seu grau de classificação;
- Comunicar prontamente à coordenação qualquer violação a esta Política, suas normas e procedimentos;
- Estar ciente de que o login de acesso ou senha à rede é pessoal e intransferível, devendo, portanto, proceder de forma responsável, garantindo o sigilo de sua senha, trocando-os de acordo com as orientações da H&P e escolhendo códigos de difícil decodificação;
- Ativar suas senhas de proteção para Correio Eletrônico (e-mail/webmail) e Sistema Operacional;
- Não executar programas que tenham como finalidade a decodificação de senhas, a monitoração da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilização de serviços;
- Não instalar ou executar programas, instalar equipamentos ou executar ações que não sejam previamente autorizados pela H&P ou que possam facilitar o acesso à rede de usuários não autorizados;
- Não fazer uso de direitos especiais de acesso ou de qualquer outro privilégio já extintos com o término do período de ocupação de cargo ou função dentro da H&P;
- Utilizar a rede corporativa de maneira profissional, ética, segura e legal, mesmo em horários de intervalo e fora do horário de trabalho;
- Buscar conhecimento necessário para a correta utilização dos recursos de hardware e software;
- Relatar prontamente à área de TI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus etc;
- Assegurar que as informações e dados de propriedade da H&P ou dos clientes e parceiros externos não sejam disponibilizados a terceiros ou utilizados para outros fins, a não ser com autorização por escrito da coordenação e do cliente;
- Respeitar áreas de acesso restrito, não executando tentativas de acesso a áreas e/ou equipamentos alheios a suas permissões de acesso;
- Relatar para a sua coordenação e à área de TI o surgimento da necessidade de um novo software para suas atividades;

- Devolver os equipamentos e recursos tecnológicos colocados à disposição pela H&P ao término do contrato de trabalho, nas mesmas condições em que recebeu;
- Responder pelo prejuízo ou dano que vier a provocar à H&P ou a terceiros em decorrência da não obediência às diretrizes e às normas aqui referidas;
- Buscar a área de TI para esclarecimentos de dúvidas referentes à esta Política.

5.2 Coordenação

- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob sua gestão;
- Orientar os colaboradores sobre os princípios e procedimentos de Segurança da Informação;
- Confirmar a compreensão e adequada assinatura do Termo de Compromisso, Sigilo e Confidencialidade dos colaboradores como condição imprescindível para que seja concedido o acesso aos ativos de informação pela H&P;
- Exigir de parceiros, prestadores de serviços e clientes a assinatura do Termo de Compromisso, Sigilo e Confidencialidade referente às informações às quais terão acesso;
- Obter aprovação técnica da área de TI antes de solicitar a compra de hardware, software ou serviços de informática;
- Elaborar, com o apoio da área da TI os procedimentos internos de segurança da informação relacionados às suas áreas, fornecendo as informações necessárias e mantendo-os atualizados;
- Informar a área de TI, sempre que necessário, atualizações referentes a processos e/ou cadastros de colaboradores para que as permissões possam ser concedidas ou revogadas de acordo com a necessidade;
- Comunicar, antecipadamente, a data de saída de colaboradores à área de TI e à outras áreas responsáveis pela disponibilização de acessos nos projetos, a fim de assegurar os procedimentos de bloqueio de acesso aos sistemas e de devolução de recursos informacionais disponibilizados;
- Notificar imediatamente a área de TI quaisquer vulnerabilidades e

ameaças à quebra de segurança;

- Contatar a área de TI se houver necessidade de uso de dispositivos externos para transporte de dados, nos termos estabelecidos pelos procedimentos internos;
- Orientar e acompanhar sua equipe no uso de arquivos locais que devem ser restritos ao mínimo necessário para a atividade em exercício, considerando eventuais limitações de acesso à internet;
- Comunicar à área de TI da necessidade de sincronizar pastas do ambiente corporativo de arquivos (SharePoint) para equipamentos, especificando o usuário o realizará e para qual finalidade;
- Assegurar treinamento para o uso correto dos equipamentos, recursos tecnológicos e sistemas de informação;
- Advertir formalmente e aplicar sanções cabíveis ao colaborador que violar os princípios ou procedimentos de segurança, relatando imediatamente o fato a área de TI.

5.3 Área de TI

- Configurar os equipamentos, sistemas e redes para cumprir os requerimentos desta Política;
- Testar a eficácia dos controles utilizados e informar ao Comitê de Informação e Privacidade e à Diretoria da H&P sobre os riscos residuais;
- Propor as metodologias e processos referentes à segurança da informação, como, avaliação de risco, análise de vulnerabilidades etc.;
- Apoiar o Comitê de Informação e Privacidade na implantação de mecanismos operacionais para suporte as atividades específicas de segurança da informação dentre as quais: classificação da informação; métodos de destruição de dados e acesso a dados em backup e correlatas.
- Analisar criticamente incidentes de segurança em conjunto com o Comitê de Informação e Privacidade, e reportar à Diretoria da H&P o ocorrido;
- Manter comunicação efetiva com o Comitê de Informação e Privacidade e com a Diretoria da H&P sobre possíveis ameaças e novas medidas de segurança;
- Restringir o acesso de colaboradores aos logs e trilhas de auditoria das

suas próprias ações, de forma a garantir que não sejam excluídos;

- Garantir segurança do acesso público e manter evidências que permitam a sua rastreabilidade para auditoria ou investigação;
- Controlar o acesso aos recursos de processamento da informação da H&P e ao processamento e comunicação da informação por colaboradores externos;
- Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes;
- Administrar, proteger e testar as cópias de segurança dos programas e dados ao negócio da H&P;
- Gerenciar o descarte de informações, em qualquer formato, a pedido dos custodiantes;
- Garantir que as informações de um usuário sejam removidas, considerando a criação de backup protegido para eventual demanda de acesso futuro, sempre autorizado pelo Comitê de Informação e Privacidade antes do descarte ou mudança de usuário;
- Planejar, implantar, providenciar e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio;
- Acompanhar pedidos do coordenador para sincronização de pastas do ambiente corporativo de arquivos (SharePoint) para equipamentos, especificando o usuário o realizará e para qual finalidade;
- Criar a identidade lógica dos colaboradores na H&P;
- Atribuir contas e senhas identificáveis aos colaboradores para uso de computadores, sistemas, bases de dados e qualquer outro ativo de informação;
- Proteger todos os ativos de informação da H&P contra códigos maliciosos e ou vírus;
- Garantir que processos de mudança não causem vulnerabilidades ou fragilidades no ambiente de produção;
- Definir as regras formais para instalação de software e hardware, exigindo o seu cumprimento dentro da H&P;
- Realizar inspeções periódicas de configurações técnicas e análise de riscos;
- Gerenciar o uso, manuseio e guarda de assinaturas e certificados digitais;

- Garantir, assim que solicitado, o bloqueio de acesso de usuários por motivo de desligamento da H&P;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso;
- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas pode ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- Monitorar o ambiente de TI, a capacidade instalada da rede e dos equipamentos, tempo de resposta no acesso à internet e aos sistemas críticos da H&P, indisponibilidade aos sistemas críticos, incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante), a atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);
- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou solicitação do coordenador ou da Diretoria;
- Orientar os colaboradores externos que utilizam redes fora dos escritórios da H&P, sobre os cuidados mínimos com a segurança da informação;
- Realizar inspeção física nas máquinas a serviço das atividades da H&P;
- Receber e conferir os recursos colocados à disposição para os colaboradores ao término do contrato de trabalho, garantindo as mesmas condições em que foram entregues para execução do trabalho;
- Gerenciar o relacionamento com os prestadores de suporte de TI;
- Promover palestras de conscientização dos colaboradores em relação à importância da segurança da informação para o negócio da H&P;
- Realizar orçamentos e aquisições de peças e serviços conforme alçadas de gastos e solicitar e monitorar as aquisições fora de alçada para o atendimento às demandas de manutenção, operação e aquisições de licenças e softwares.

5.4 Comitê de Informação e Privacidade

- Propor metodologias, sistemas e processos específicos que visem a aumentar a segurança da informação, privacidade e proteção de dados pessoais;
- Promover a conscientização dos colaboradores em relação à importância da segurança da informação, privacidade e proteção de dados pessoais;
- Propor investimentos relacionados à segurança da informação, privacidade e proteção de dados pessoas com o intuito de minimizar os riscos;
- Gerir o Programa de Privacidade da H&P, conforme disposto na Política de Privacidade e Proteção de Dados Pessoais;
- Classificar e reclassificar o nível de acesso às informações sempre que necessário;
- Analisar criticamente incidentes de segurança em conjunto com a área de TI e reportar à Diretoria da H&P o ocorrido;
- Sugerir e cobrar novas medidas de segurança, ações de correções, novas definições e procedimentos pela área de TI, a partir da ciência de riscos residuais em controles utilizados, ocorrência de incidentes de segurança e possíveis ameaças;
- Manter comunicação efetiva com a área de TI e com a Diretoria da H&P sobre possíveis ameaças e novas medidas de segurança;
- Apoiar a avaliação e a adequação de controles de segurança da informação para novos sistemas ou serviços;
- Buscar alinhamento com as diretrizes corporativas da Herkenhoff & Prates;
- Revisar essa Política, bem como a Política de Privacidade e Proteção de Dados Pessoais a cada 1 ano ou, se necessário, quando houver algum incidente de segurança da informação, privacidade ou proteção de dados pessoais e consequente mudança de procedimentos e normas;
- Comunicar aos colaboradores qualquer mudança nos procedimentos de controles que possam afetar a execução do seu trabalho, a segurança da informação, privacidade e proteção de dados pessoais.

6. CONTROLES DE ACESSOS

6.1 Acesso à rede corporativa

- A rede H&P e os equipamentos que a compõem têm como finalidade única e exclusiva permitir aos seus colaboradores a prática de atividades relacionadas ao trabalho, à pesquisa e à disseminação de informações de interesse da H&P e de suas unidades;
- Têm direito de uso da rede os colaboradores e demais usuários autorizados pela H&P e por suas unidades;
- O uso da internet, acesso à rede e criação de ID de usuário e de e-mail corporativo (usuário@hpconsultores.com.br) serão previamente autorizados pela H&P ou por seus representantes através de comunicação à área de TI;
- O ID de usuário de acesso à rede, bem como sua senha e demais acessos a sistemas são pessoais e intransferíveis;
- Tudo que for executado com a senha de usuário da rede ou de sistema será de inteira responsabilidade do usuário;
- Todos os acessos e serviços disponíveis serão monitorados pela H&P para assegurar o cumprimento das diretrizes previstas nesta Política, prevenir perdas/extravios e proteger as informações da empresa e dos profissionais colaboradores, mantendo as garantias de sigilo corporativo e pessoal requeridas pela legislação vigente;
- Quando o colaborador utilizar dispositivos de sua propriedade como ferramenta de trabalho na H&P, seu uso será disciplinado, no que couber, por esta Política; zelando sempre pela segurança da informação.

6.2 Login e senha

- Os usuários devem ter identificação única com a finalidade de distinguir seus acessos, rastreabilidade de atividades realizadas e estabelecer as respectivas responsabilidades;
- A senha de todos os usuários deverá ser definida, alterada e bloqueada, conforme critérios, regras e prazos definidos pelo mecanismo de autenticação em uso. Atualmente, a H&P realiza a

autenticação de seus usuários por meio do software Microsoft Azure;

- A H&P poderá utilizar-se de mais de uma solução de informação que exija senhas; devendo o colaborador estar atento as especificidades de cada solução;
- As senhas são efetivas apenas quando usadas corretamente e sua escolha e uso requerem alguns cuidados como:
    - Senhas temporárias devem ser alteradas imediatamente, e não devem ser armazenadas de forma desprotegida;
    - Utilizar um método próprio para lembrar da senha, de modo que ela não precise ser escrita em nenhum local, em hipótese alguma;
    - Na criação de senhas não é permitido utilizar informações pessoais fáceis de serem obtidas, como o número de telefone, nome da rua, nome do bairro, cidade, data de nascimento etc.
- Todas as operações e tentativas de login são registradas, monitoradas e protegidas de adulteração pela área de TI da H&P, estando sujeitas a auditorias;
- Quaisquer problemas de acesso deverão ser notificados imediatamente à coordenação e à área de TI.

6.3 Acesso ao correio eletrônico (E-mail e Webmail)

- O correio eletrônico é de propriedade da H&P e todos os usuários estão sujeitos ao monitoramento do conteúdo de suas caixas postais, bem como, tráfego de mensagens, histórico de utilização, bloqueio de mensagens com conteúdo inadequado e/ou com vírus e códigos maliciosos (spam, phishing etc.);
- Todos os colaboradores da H&P deverão utilizar seu e-mail e webmail corporativo (usuário@hpconsultores.com.br) exclusivamente para realização de suas atividades profissionais;
- O uso do e-mail e webmail corporativo requer alguns cuidados como:
    - Acessar com frequência o e-mail e webmail corporativo, a fim de se informar sobre as atividades da H&P;
    - Manter a conta de e-mail e webmail atualizada, evitando acúmulo de e-mails e arquivos desnecessários, observando a cota máxima de e-mails armazenados, estipulada e gerenciada

pela área de TI;

- Eliminar imediatamente mensagens recebidas de origem desconhecida após sua pré-visualização, sem leitura de seu conteúdo, para evitar contaminação por vírus e outros riscos;
- Utilizar o padrão para o corpo do texto e assinatura dos e-mails de acordo com instruções encaminhadas pela área de Comunicação;
- Não utilizar o e-mail e webmail corporativo da H&P para o envio ou recebimento de mensagens não relacionadas ao trabalho, correntes, spams ou e-mails enviados em grande quantidade e/ou para vários destinatários que não sejam solicitados ou autorizados pela empresa. É proibido utilizar o e-mail corporativo para reenviar ou propagar mensagens em cadeia, correntes ou pirâmides, independente da vontade do destinatário de receber tais mensagens;
- Não utilizar o e-mail e webmail corporativo da H&P para o envio de mala direta, publicidade, material comercial, anúncios, informativos, campanhas ou propagandas que não tenham sido previamente solicitados ou autorizados pela empresa;
- Não fornecer ou cadastrar o e-mail e webmail corporativo da H&P em sites de propaganda, redes sociais, notícias, compras ou qualquer outro site que não seja de total interesse e autorizado pela empresa;
- Não alterar quaisquer das informações do cabeçalho do remetente;

- O uso indevido do e-mail e webmail é de inteira responsabilidade do usuário, podendo o mesmo ser responsabilizado por eventuais danos causados;
- Em nenhuma hipótese a H&P será responsabilizada perante quaisquer usuários ou terceiros pela perda de mensagens e/ou respectivo conteúdo;
- Caso o Comitê de Informação e Privacidade julgue necessário, as seguintes ações poderão ser tomadas pela área de TI:
  - Bloqueio de e-mails com arquivos anexos que comprometam a segurança, o uso da rede ou o andamento das atividades relacionadas ao trabalho;

- Bloqueio de e-mails para destinatários ou domínios que comprometam a segurança, o uso da rede ou o andamento das atividades relacionadas ao trabalho;
- Bloqueio de e-mails para vários destinatários, ou que possam caracterizar o domínio hpconsultores.com.br como propagador de spam.

6.4 Utilização da internet e redes/mídias sociais

- O acesso à internet é uma concessão para fins profissionais e não um direito pessoal. Portanto, sua utilização, deve ser exclusivamente para atividades ligadas ao trabalho.
- Não é permitido o acesso indiscriminado a redes/mídias sociais. Sua utilização, deve ser exclusivamente para atividades ligadas ao trabalho.
- O uso indevido do acesso à internet é de inteira responsabilidade do usuário, que pode ser responsabilizado legalmente por eventuais danos causados;
- É terminantemente proibida utilização do acesso à internet e acesso a redes/mídias sociais e seus recursos referentes à jogos, conteúdo adulto ou ofensivo, apologia ao uso de drogas, intolerância racial ou religiosa, incitação à violência, atividades criminosas e fraudes.
- Não utilizar a rede para fazer downloads ou uploads não autorizados ou não relacionados às atividades da H&P ou que não sejam previamente autorizados.

6.5 Utilização de aplicativos de mensagens instantâneas e videoconferências

- A troca de mensagens instantâneas e realização de videoconferências de caráter interno ou externo com colaboradores da H&P deve ser realizada por meio do aplicativo padrão Microsoft Teams;
- Excepcionalmente, é permitido aos colaboradores utilizar outros aplicativos não-padrão de mensagem instantânea (Whatsapp, Telegram ou correlatos) ou de videoconferência (Zoom, Google Meet ou correlatos) para fins corporativos, somente quando necessário ou quando este for o único meio para promover a troca de informações;

desde que a troca de mensagens não contenha assuntos e/ou arquivos sigilosos, confidenciais, dados pessoais e/ou dados pessoais sensíveis;

- Em grupos criados para discussão de temas relacionados às atividades da empresa, devem restringir o conteúdo das mensagens aos assuntos corporativos;
- Recomenda-se o uso de filtro de fundo de tela padronizado em reuniões externas, especialmente as que contarem com a participação de clientes e parceiros;
- Deve-se respeitar os horários regulamentares de folga dos demais colaboradores, fazendo contato fora do horário de trabalho apenas quando estritamente necessário.

6.6 Acesso privilegiado

- A utilização de acessos privilegiados a servidores, bancos de dados específicos, diretórios, bem como outros softwares e programas selecionados; é restrita a colaboradores previamente autorizados pela H&P;
- O acesso privilegiado pode ser concedido pelo coordenador de acordo com as atividades desenvolvidas pelo colaborador, mediante comunicação com área de TI;
- O controle de acessos privilegiados é de responsabilidade dos coordenadores juntamente com a equipe de TI;
- É proibido compartilhamento de dados de acesso privilegiado com colaboradores não autorizados.

6.7 Acesso à captura remota de estação de trabalho

- Não é permitido o acesso indiscriminado interno e/ou externo para captura remota de estação de trabalho para todo o público de colaboradores;
- O acesso à captura remota de estação de trabalho pode ser liberado pelo próprio usuário e/ou mediante aprovação do seu coordenador ou da Diretoria através de formalização via e-mail para a área de TI.

6.8 Acesso a redes sem fio (corporativa/visitantes)

- A utilização dos recursos de redes sem fio é uma solução tecnológica complementar aos demais recursos de TI previstos nesta política, portanto, todas as diretrizes previstas nesta Política devem ser observadas e cumpridas em sua utilização;
- Somente os colaboradores que receberem equipamentos da H&P terão o acesso pré-aprovado a rede sem fio corporativa da H&P, exclusivamente para fins profissionais no tratamento de informações corporativas;
- Os colaboradores que fizerem uso de equipamentos particulares para a execução de suas atividades profissionais (colaborador sem equipamento da empresa ou prestador de serviço com equipamento do fornecedor), podem ter acesso a rede sem fio corporativa da H&P mediante aprovação do coordenador ou da Diretoria, definindo-se quantidade de dispositivos e finalidade de uso, observando dispositivos da seção 7.3 "Uso aceitável dos equipamentos" desta Política;
- O acesso obtido pelo usuário de rede sem fio deve ser utilizado exclusivamente para os fins que foi aprovado, portanto, está vedada a possibilidade de aproveitar a liberação do recurso para também realizar outro tipo de acesso similar que não foi previsto e aprovado.

6.9 Acesso a conteúdo de TI de profissional desligado, afastado e investigado

- Não é permitido o acesso indiscriminado ao conteúdo de TI de profissionais desligados, afastados e investigados por demais colaboradores;
- O acesso a conteúdo de TI (arquivos armazenados na estação de trabalho, no perfil do Windows, conteúdo de caixa postal/e-mails etc.) de um colaborador desligado, afastado ou investigado é previsto considerando que a produção do profissional é de propriedade da empresa, portanto, poderá ser acessado exclusivamente para fins profissionais, a fim de identificar e tratar atividades pendentes, e investigar eventuais cenários de fraude ou comportamento inadequado perante o Código de Conduta e/ou a esta Política;

- A solicitação de acesso a este tipo de conteúdo poderá ser liberada preferencialmente ao coordenador mediante aprovação da diretoria exclusivamente para solicitantes que possuam cargos com subordinação direta somada a da Segurança da Informação, e sempre que houver necessidade o aprovador poderá delegar sua função por limitação tecnológica ou inviabilidade de atendimento local da demanda;
- O direito de uso da rede cessa quando o usuário encerrar seu vínculo regular com a H&P, seja através do desligamento por qualquer motivo, suspensão do contrato de trabalho ou serviço prestado ou pelo encerramento de atividades que justifiquem seu acesso à rede;
- Como parte do procedimento de desligamento do funcionário a TI, ao ser notificada, deverá realizar a troca da senha do usuário, bloqueando o acesso ao computador e dados na nuvem, bem como, fazer o backup de todos dados do OneDrive e todos os documentos existentes do computador e ainda gerar um arquivo PST de todos os e-mails para um armazenamento em servidor local ou na nuvem;
- Caso o usuário venha a exercer nova atividade relacionada à H&P após o encerramento do vínculo regular, deverá ter sua autorização de uso da rede e acessos revistos, não podendo fazer uso dos direitos que lhe foram concedidos em situação anterior.

7. GESTÃO DE ATIVOS DE INFORMAÇÃO

7.1 Inventário de ativos

- Para controle de ativos de informação da H&P a área de TI deve manter um inventário junto com os coordenadores;
- Cada área deve adicionar no inventário de ativos seu fluxo de informações geradas no decorrer de suas atividades, seguindo o ciclo de vida da informação, sendo eles:
    - Nome do ativo;
    - Data de criação;
    - Local de armazenamento;
    - Data de exclusão/destruição;
    - Método de transferência;

- Colaborador-controlador e colaborador-operador responsável;
- Classificação do ativo;
- Área/colaborador com permissão sob o arquivo;

7.2 Gestor de ativos

O gestor de ativos é o coordenador, que deverá gerenciar os ativos de seu fluxo de atividades na H&P, assegurando que:

- Estão sendo inventariados;
- Classificados e protegidos;
- Aderentes aos padrões desta Política;
- Sendo corretamente destruídos ou excluídos;

7.3 Uso aceitável dos equipamentos

- A H&P fornecerá aos seus colaboradores os equipamentos necessários para a execução de suas atividades de trabalho quando necessário;
- O colaborador é responsável pelo seu equipamento e todos os dados e informações nele tratados;
- Deverá haver um controle dos equipamentos adquiridos e descartados pela H&P;
- A área de TI deverá realizar periodicamente o levantamento e promover a adequação dos equipamentos da H&P que eventualmente estejam em desacordo com os softwares licenciados;
- Toda movimentação e manutenção de equipamentos da H&P deverá ser realizada pela área de TI através de solicitação formalizada;
- A permissão para uso de equipamentos particulares na execução das atividades pelos colaboradores está a critério único e exclusivo da H&P. O colaborador deverá estar formalmente autorizado e concordar integralmente com as diretrizes desta Política, antes de se fazer uso de seus dispositivos na infraestrutura ou manusear dados e informações da H&P;
- A H&P não se responsabilizará pelo suporte, atualização, manutenção, reposição de peças, licenciamento de softwares, reembolso ou cobrir qualquer tipo de custo referente ao uso de equipamentos particulares;
- Quando autorizado o uso de equipamentos particulares para

execução das atividades da H&P, o colaborador será inteiramente responsável por garantir a segurança de seus dispositivos, garantindo que:

- O sistema operacional estará com as últimas atualizações de segurança aplicadas;
- Possuir software antivírus com assinaturas e varreduras em dia;
- Possuir softwares licenciados, preservando o direito autoral;
- Remover softwares que possam prejudicar a segurança da infraestrutura da H&P;
- Evitar salvar senhas no navegador, anotações em arquivos de texto ou bilhetes;

- Todos os colaboradores e partes externas devem devolver todos os ativos da H&P que estejam em sua posse após o encerramento de suas atividades, do contrato ou acordo sob pena de adoção de providências administrativas e judiciais.

7.4 Uso aceitável dos ativos de informação

- A H&P utiliza o SharePoint como repositório central para armazenamento de todos os arquivos produzidos no exercício de suas atividades;
- Todos os arquivos contidos no SharePoint devem ser exclusivamente de interesse da H&P. É proibida a criação de pastas pessoais nos servidores de rede;
- O uso ou armazenamento de dados em equipamentos particulares não altera a propriedade intelectual da H&P sobre os dados e as informações criados, armazenados, enviados, recebidos, modificados ou excluídos;
- O colaborador dispõe de espaço de armazenamento individual no OneDrive for Business como alternativa segura para produzir ou salvar arquivos temporários, que não são as versões finais dos produtos dos serviços;
- A criação de pastas departamentais ou de projetos nos servidores de rede e SharePoint deverá refletir a estrutura organizacional da H&P ou da execução dos projetos, respectivamente, e ser solicitada ao responsável pela área de TI;

- O acesso às pastas departamentais ou de projetos no servidor da H&P e SharePoint exige autorização do coordenador e da área de TI, que garante o controle do acesso de cada usuário;
- Os colaboradores da H&P devem assegurar que estão mantendo as informações em utilização e armazenamento nos caminhos corretos dentro da estrutura hierarquizada de cada equipe que possuem acesso;
- A sincronização de pastas do ambiente corporativo de arquivos (SharePoint) para equipamentos, é procedimento restrito a colaboradores autorizados pelo coordenador e acompanhados pela área de TI. O pedido de realização desse procedimento deve conter justificativa baseada na finalidade da sincronização;
- Para o compartilhamento de arquivos de trabalho salvos no SharePoint ou no OneDrive for Business entre colaboradores, é recomendado que a utilização da função compartilhar arquivo, sendo possível também a criação de links com acesso limitado a membros da corporação;
- O compartilhamento de arquivos com clientes e parceiros deverá observar as regras estabelecidas na seção 8.1 "Procedimentos gerais de segurança das operações" desta Política, levando em consideração a finalidade do compartilhamento, a classificação da informação e o meio ou software de utilizado;
- O uso de dispositivos móveis de armazenamento (pendrives, HDs, DVD's etc) será autorizado aos colaboradores em virtude de suas atividades profissionais mediante liberação de transporte pelo coordenador e formalização a área de TI da H&P, contendo:
    - Descriminação de finalidade do transporte;
    - Descriminação do prazo de transporte;
    - Instruções para descarte das informações;
- O coordenador será corresponsável pelo procedimento de transporte de informações em dispositivos móveis, garantindo o descarte adequado das informações no prazo determinado;
- É proibida a produção e armazenamento de arquivos de trabalho em nuvens não corporativas (OneDrive particular, Dropbox, Google docs etc) e nas próprias máquinas;
- É proibido o compartilhamento de arquivo de trabalho em nuvens não corporativas (OneDrive particular, Dropbox, Google docs etc);

- Não é permitida a utilização ou o acesso indiscriminado a dispositivos móveis de armazenamento de informações nos equipamentos da H&P;
- O descarte de arquivos digitais salvos nos equipamentos deverá ser total, procedendo com a imediata limpeza de pastas de lixeira local e com a destruição de quaisquer cópias de backup ou transporte para eventuais atividades em áreas sem acesso à internet;
- Os HDs e pendrives deverão ser encaminhados à área de TI para a destruição da informação ou backup antes do descarte ou reutilização;
- Informações sensíveis ou confidenciais, quando impressas em local coletivo, devem ser retiradas da impressora imediatamente;
- Quaisquer mídias ou documentos impressos contendo informações de propriedade da H&P deverão ser destruídas antes de seu descarte.

7.5 Classificação da informação

- Para a classificação da informação deverá ser levado em conta o valor, requisitos legais, sensibilidade e criticidade para a H&P, para evitar modificação ou divulgação não autorizada;
- A definição de palavras-chave, de metadados, de nomenclatura de arquivos e de pastas no servidor e nuvens corporativas deve seguir as instruções de padronização definidas pela H&P, conforme procedimento interno;
- As informações devem ser classificadas e identificadas no momento de sua criação pelo colaborador de acordo com os seguintes níveis:
    - **Pública:** Informações com baixo ou nenhum nível de risco, que não comprometem as atividades da H&P, e que, por isso, não precisam de proteção efetiva ou tratamento específico, passível de exposição para terceiros;
    - **Interna:** Informações disponíveis aos colaboradores da H&P para a execução de suas atividades rotineiras, não se destinando, por tanto, ao público externo;
    - **Confidencial:** Informações de acesso restrito a um colaborador ou grupo de colaboradores. Sua revelação pode violar a privacidade de indivíduos, violar acordos de confidencialidade, dentre outros. Todos os documentos que contenham dados pessoais ou dados pessoais sensíveis devem ser classificados

como confidencial;
    - **Confidencial restrita:** Informações de acesso restrito associadas ao interesse estratégico da H&P, restritas a Diretoria, coordenações de área e colaboradores cujas funções requeiram conhecê-las;
- A H&P disponibiliza modelos dos documentos eletrônicos oficiais, que estão rotulados e aderentes aos padrões da organização; e devem ser utilizados nas documentações oficiais da H&P, isto é, possuem em seu corpo:
    - Logo da organização;
    - Classificação;
    - Palavras-chave e metadados;
    - Versão do documento.

8. SEGURANÇA FÍSICA E DO AMBIENTE

8.1 Acesso físico

O acesso físico deve ser controlado e orientado de maneira a disciplinar a movimentação e circulação de pessoas, materiais, equipamentos e veículos, nos termos dos procedimentos internos.

9. SEGURANÇA NAS OPERAÇÕES

9.1 Procedimentos gerais de segurança das operações

- Com a finalidade de garantir a operação segura e correta dos recursos de processamento da informação, a H&P compromete-se a manter rigoroso controle de seus procedimentos de operação, por meio de documentação. O Comitê de Informação e Privacidade, juntamente com a área de TI, o encarregado da H&P ("DPO") e os coordenadores são responsáveis pela execução dessas atividades;
- Toda mudança na estrutura de segurança da informação da H&P, em seus processos de negócio, em seu processamento da informação e nos sistemas que afetam a segurança da informação deverão ser controlados pela H&P;

- A alteração dos parâmetros de infraestrutura dos recursos de TI por pessoas que não estejam devidamente credenciadas ou autorizadas para tal implica em conduta que viola a política da H&P, caracterizando motivo de medida disciplinar;
- A utilização dos recursos deverá ser monitorada e ajustada periodicamente pela área de TI e a projeção de recursos deverá ser feita para necessidades de capacidade futura para garantir o desempenho requerido do sistema da H&P;
- Os softwares instalados nos equipamentos da H&P e servidor de rede são de propriedade exclusiva da H&P; sendo proibidas as cópias integrais ou parciais, bem como a instalação de softwares piratas. A instalação de softwares não autorizados (Pirataria) constitui crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/98, e o infrator está sujeito à pena de detenção e multa;
- Toda aquisição de novo software deverá ser avaliada previamente pela área de TI da H&P mediante emissão de parecer, observados os requisitos mínimos de segurança da informação aderentes à LGPD, esta Política e demais procedimentos que tratarem do assunto;
- Todos os equipamentos disponibilizados pela H&P ou autorizados por ela a acessar sua infraestrutura deverão possuir ferramenta de antivírus instalado como medida de prevenção contra malware;
- Periodicamente os colaboradores podem ser submetidos a auditorias nos equipamentos que utilizam. Tais ações são necessárias para que sejam validadas as conformidades com a PSI e às regras de utilização dos recursos de informática da H&P;
- Os acessos à infraestrutura da H&P devem ser gerenciados ao ponto de evitar que terceiros tenham acesso não autorizado aos recursos da organização, utilizando ferramentas de monitoramento e controle na utilização de recursos da rede;
- As transferências de dados entre colaboradores e clientes devem utilizar canais oficiais de comunicação:
    - Por meio de anexo encaminhado entre e-mails corporativos observando o estabelecido em contrato;
    - Por meio de transferência com acesso controlado por login em plataforma da H&P;
    - Por meio de link de acesso restrito, conforme estabelecido em

contrato, observando as permissões do servidor;
    - Por meio de link público de acesso, conforme estabelecido em contrato, mediante a assinatura de termo de responsabilização por parte do cliente;
- A entrega de informações e dados sensíveis para clientes será realizado por meio de transferência com acesso controlado por login. Tais ações devem ser monitoradas e validadas quando outros meios de transferência ou comunicação forem requeridos;
- Durante a operação dos sistemas e execução de projetos, as áreas da H&P deverão garantir os requisitos de confidencialidade, integridade, disponibilidade e privacidade, baseadas no conceito de privacidade incorporada aos processos (Privacy by Design e Privacy by Default), além de outras boas práticas usadas no mercado, nos moldes dos procedimentos internos.

9.2 Requisitos de segurança da informação e privacidade no tratamento e desenvolvimento

- Os colaboradores que, no exercício de suas funções, realizarem qualquer tipo de tratamento de dados pessoais sensíveis ou não, ou desenvolvimento deverá ter como premissa os princípios da segurança da informação e da privacidade dispostas nesta Política e na Política de Privacidade e Proteção de Dados da H&P;
- Na realização de quaisquer procedimentos de tratamento, incluindo a pesquisa e coleta de dados, os colaboradores deverão verificar as permissões de uso dos dados da fonte de origem, bem como cumprir os princípios da LGPD, desta Política e da Política de Privacidade e Proteção de Dados da H&P;
- Ambientes de desenvolvimento, teste e produção deverão ser separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção;
- O colaborador responsável por desenvolvimento deverá submeter periodicamente o sistema a testes de validação de código e funcionalidade para garantir a disponibilidade e integridade durante o processamento das informações;
- Devem ser observadas as interfaces utilizadas para administração do

sistema e operação, adicionando proteções adequadas nos dispositivos que possam afetar a disponibilidade, integridade, confidencialidade e privacidade dos dados;

9.3 Backup de arquivos

- A H&P conta com sistema de cópias de segurança (backups) centralizado na nuvem do Sharepoint, não sendo permitida a realização de cópias de segurança em outros ambientes. Qualquer necessidade de realização de backup local deverá ser tratada diretamente com a área de TI;
- Compete à área TI estabelecer regras e auditar o serviço contratado para a realização de cópias de segurança (backups);
- Todos os arquivos que estiverem armazenados na SharePoint ou OneDrive for Business estão resguardados por backup automático, além de controle de versionamento e responsáveis pelas alterações;
- Em caso de perda de dados em razão de erro do backup automático, o colaborador deverá acionar a respectiva coordenação, bem como ao Comitê de Informação e Privacidade que elaborará estratégia específica para restauração do arquivo.

10.SEGURANÇA NAS COMUNICAÇÕES

10.1 Acesso à criação e utilização de diretórios e grupos de distribuição de e-mails

- Não é permitida a criação e utilização indiscriminada de diretórios e/ou grupos de distribuição de e-mails para utilização interna e/ou externa para todo o público de colaboradores da H&P;
- A solicitação de criação e/ou acesso a um grupo de distribuição de e-mails pode ser liberada mediante aprovação do coordenador ou pela Diretoria, mediante formalização a área de TI.

10.2 Telas e mesas limpas

- Os computadores deverão ser bloqueados quando não estiverem sendo utilizados. Quando o computador ficar em stand-by por mais de

cinco minuto, a sessão será finalizada, solicitando login e senha novamente ao usuário;

- O papel de parede de todos os equipamentos deverá seguir a padronização da H&P;
- Os documentos em papéis e mídias eletrônicas, em especial, contendo informações sensíveis ou críticas, devem ser armazenados em armários ou gavetas trancadas quando não estiverem em uso;
- Ao final do expediente, ou em caso de ausência prolongada do local de trabalho, a mesa de trabalho deve permanecer limpa, documentos guardados, gavetas e armários trancados e computador bloqueado ou desligado;
- Preferencialmente, mesas e móveis deverão ser posicionados de forma que dados sensíveis não sejam visíveis de janelas ou corredores;
- Não deixar o local de trabalho aberto sem que haja um colaborador que trabalhe no local presente;
- Anotações, recados, lembretes e quaisquer informações sensíveis não devem ser deixados à mostra em quadros, sobre a mesa ou colados em paredes, divisórias, murais ou monitor do computador.

11. GESTÃO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

- O Comitê de Informação e Privacidade, juntamente com a área de TI, são responsáveis pela gestão de incidentes de segurança da informação, realizando, periodicamente, mapeamento e identificação de possíveis riscos para elaboração de planos de ação visando sua mitigação, de acordo com procedimentos internos. O encarregado da H&P (“DPO”) e os coordenadores são responsáveis por auxiliar na execução dessas atividades;
- Todos os colaboradores da H&P no exercício de suas funções são responsáveis por mitigar e denunciar possíveis incidentes de segurança da informação, agindo de acordo com essa Política e outras normas e procedimentos internos para esse fim;
- Observada fragilidade, suspeita ou evidência de incidente de segurança da informação, o colaborador da H&P deverá notificar o

Comitê o mais rápido possível;

- Os conhecimentos obtidos da análise e resolução dos incidentes de segurança da informação deverão ser utilizados pela H&P para reduzir a probabilidade ou o impacto de incidentes futuros.

12. AUDITORIAS

- As auditorias e a emissões de relatórios serão realizadas periodicamente ou sempre que solicitado pela Diretoria, área de TI ou profissional contratado para esse fim, com o objetivo de observar o cumprimento das normas desta Política pelos colaboradores e com vistas à gestão de desempenho e segurança da informação;
- A Diretoria da H&P poderá solicitar, à área de TI, relatórios de auditoria contendo o nome, mensagens trafegadas, acessos à internet e demais informações do usuário, conforme resolução do TST – Tribunal Superior do Trabalho;
- Havendo evidência de atividade que possa comprometer a segurança da rede ou que descumpra as regras estabelecidas por esta Política, será permitido ao administrador da rede auditar e monitorar as atividades de um usuário, além de inspecionar seus arquivos, registros de acesso, contas de e-mail corporativo e acesso aos sistemas e sites de comunicação interna da H&P, sendo o fato imediatamente comunicado à Diretoria ou seus representantes. Os dados apurados no computador serão mantidos em sigilo pela direção da H&P;
- A H&P poderá, a qualquer tempo, implantar aplicativos de segurança, monitoramento e registro do uso da rede e internet, instalar softwares e hardwares para proteger a rede e garantir a integridade dos dados e programas, instalar firewall, inspecionar arquivos armazenados na rede, seja em disco local, virtual ou nas áreas privadas da rede, a fim de assegurar o cumprimento das regras aqui estabelecidas;
- A privacidade e proteção das informações de identificação pessoal devem ser asseguradas conforme requerido por legislação e regulamentação pertinente, quando aplicável.

13. COMUNICAÇÃO, TREINAMENTO E DÚVIDAS

A H&P manterá um plano de comunicação e treinamento periódico e constante para seus Colaboradores com intuito de divulgar e conscientizar da importância do cumprimento das regras dessa Política.

É de responsabilidade de todos os coordenadores da H&P divulgar para aos colaboradores sob sua gestão o conteúdo desta Política e conscientizá-los sobre a necessidade e importância de sua observância e incentivá-los a apresentar dúvidas com relação a sua aplicação.

14. COMITÊ DE INFORMAÇÃO E PRIVACIDADE

Fica instituído no âmbito da H&P a criação do Comitê de Informação e Privacidade ("Comitê"), responsável por validar, monitorar e salvaguardar os princípios corporativos de segurança da informação, privacidade e proteção de dados, de acordo com seu regimento interno.

O Comitê será composto por 5 (cinco) membros, representantes da Diretoria, do setor Administrativo, do setor de Negócios e Relações Institucionais, do setor de Gestão de Dados e do setor de Projetos da H&P, indicados pela Diretoria de acordo com os requisitos de idoneidade moral, reputação ilibada e notórios conhecimentos das atividades executadas pela H&P.

Cada setor representado no Comitê contará com 1 (um) suplente, que assumirá as responsabilidades do indicado em caso de impossibilidade de exercer o cargo.

O mandato de seus membros será de 2 (dois) anos, permitida recondução.

O Comitê deverá se reunir formalmente a cada 90 (noventa) dias e, extraordinariamente, sempre que for necessário, para apresentação e acompanhamento do Programa de Privacidade, bem como para deliberar sobre algum incidente grave ou definição relevante para a H&P.

15. DISPOSIÇÕES FINAIS

- Qualquer colaborador, terceiro ou parceiro que viole qualquer disposição desta Política estará sujeito as medidas disciplinares previstas no Código de Conduta da H&P, em observância a legislação aplicável, em especial:
    - Advertência por escrito;
    - Suspensão;
    - Dispensa sem justa causa;
    - Dispensa por justa causa;
    - Exclusão do fornecedor ou parceiro;
    - Remoção do recurso envolvido;
    - Ação judicial cabível.
- Deverão ser considerados na aplicação das medidas disciplinares fatores como função exercida pelo colaborador, período utilizado, local de utilização, horário de utilização, prejuízo real ou potencial causado à H&P.

HISTÓRICO DE REVISÕES

DATA	REVISÃO	DESCRIÇÃO	REVISADO POR
-	30/06/2021	Revisão e adequação as exigências da LGPD	Jacqueline Torres Juliana Aschar
02/06/2017	-	Criação da Política	Diretoria da H&P

ANEXO I – GLOSSÁRIO

- **Acesso:** ato de ingressar, transitar, conhecer ou consultar a informação, bom como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique.
- **Acesso privilegiado:** É a utilização de uma conta de acesso, cujo conjunto de privilégios fornece poderes de administração de um determinado sistema, de maneira ampliada.
- **Acesso restrito:** é a utilização de uma conta de acesso, cujo conjunto de privilégios fornece poderes de administração de um determinado sistema, de maneira ampliada, porém sua senha não pode ser alterada e de utilização restrita.
- **Acesso remoto:** Consiste na capacidade de um computador acessar, à distância, um outro computador ou de uma rede de computadores e, assim, visualizar arquivos, o desktop e até controlar programas e as funcionalidades dos dispositivos acessados.
- **Agente de tratamento de dados pessoais**: É o colaborador que em suas atividades exerce função de controlador ou operador de dados pessoais nos termos da LGPD.
- **Análise de incidentes:** Consiste em examinar todas as informações disponíveis sobre o incidente, incluindo artefatos e outras evidências relacionadas ao evento. O propósito dessa análise é identificar o escopo do incidente, sua extensão, sua natureza e quais prejuízos causados. Também faz parte da análise de incidente propor estratégias de contenção e recuperação.
- **Análise de riscos:** Uso sistemático de informações para identificar fontes e estimar riscos.
- **Ativo:** Qualquer coisa que tenha valor para a H&P.
- **Ativo da informação:** São os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, bem como os recursos humanos que a eles têm acesso.
- **Auditoria:** Processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em

conformidade) à consecução dos objetivos.

- **Autenticação:** Processo que busca verificar a identidade digital de uma pessoa ou entidade quando ela requisita acesso a um sistema. O processo é realizado por meio de regras preestabelecidas, geralmente pela comparação das credenciais apresentadas pela entidade com outras já pré-definidas no sistema, reconhecendo como verdadeiras ou legítimas as partes envolvidas em um processo.
- **Autenticidade**: É a certeza de que a fonte da informação é verdadeira, que não sofreu nenhuma alteração ao longo da sua fluidez. Qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema.
- **Backup** ou **Cópia de segurança**: Conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada.
- **Banco de dados**: Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
- **Bloqueio:** Suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do bando de dados;
- **Código malicioso:** Programa, ou parte de um programa de computador, projetado especificamente para atentar contra a segurança de um sistema computacional, normalmente através de exploração de alguma vulnerabilidade de sistema.
- **Colaboradores:** São todos os empregados, diretores, estagiários, menores aprendizes, empregados temporários, autônomos e demais indivíduos que mantém algum vínculo permanente ou temporário de trabalho com a Herkenhoff & Prates.
- **Confidencialidade:** Garante a proteção das informações, permitindo que sejam acessadas apenas por indivíduos autorizados, comprovada a necessidade do acesso e o nível de responsabilidade do colaborador.
- **Controle de acesso:** Conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação.
- **Controlador de dados pessoais** ou **Colaborador-Controlador:** Pessoa

física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

- **Dados pessoais:** Informação relacionada a pessoa natural identificada ou identificável. Também são considerados dados pessoais aqueles utilizados para formação do perfil comportamental de determinada pessoa natural.
- **Dados pessoais sensíveis:** Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico quando vinculado a pessoa natural.
- **Disponibilidade**: Qualidade da informação que pode ser conhecida, acessada e utilizada por indivíduos, equipamentos ou sistemas autorizados sempre que necessário.
- **Eliminação:** Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.
- **Encarregado ou *Data Protection Officer* ("DPO"):** Pessoa física ou jurídica indicada pelo Agente de Tratamento para atuar como canal de comunicação entre o Controlador, os titulares de dados e a ANPD.
- **Fornecedores:** São considerados fornecedores os outros terceiros contratados e subcontratados, pessoa física ou jurídica, não enquadrados como parceiros comerciais.
- **Gestão de riscos:** Processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar, e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.
- **Gestão de segurança da informação:** Ações e métodos que visam à integração das atividades de gestão de riscos, à gestão de continuidade do negócio, ao tratamento de incidentes, ao tratamento da informação, à conformidade, ao credenciamento, à segurança cibernética, à segurança física, à segurança lógica, à segurança orgânica e à segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações.

- **Incidente:** Evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.
- **Incidente de segurança:** Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.
- **Informação confidencial**: Toda e qualquer informação de qualquer natureza - técnica, operacional, comercial e jurídica -, incluídas em descrição ou documentos que envolvam o know-how da empresa, planos de negócios, métodos de contabilidade, técnicas e experiências acumuladas, documentos técnicos e administrativos, contratos, papéis, estudos, pareceres, pesquisas, transmitidas pela empresa ao(a) colaborador(a) ou por ele(a) coletada.
- **Lei Geral De Proteção De Dados ("LGPD")**: Diploma normativo (Lei nº 13.709, de 14 de agosto de 2018) que dispõe sobre o tratamento de dados pessoais em meios digitais ou físicos realizados por pessoa natural ou por pessoa jurídica, de direito público ou privado, tendo como objetivo defender os titulares de dados pessoais e ao mesmo tempo permitir o uso dos dados para finalidades diversas, equilibrando interesses e harmonizando a proteção da pessoa humana como desenvolvimento tecnológico e econômico.
- **Integridade da informação:** Qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino. Significa dizer que as informações devem ser armazenadas da mesma forma que foram fornecidas, sem qualquer alteração em seu conteúdo e mantidas em seu formato original e verdadeiro, a fim de servir para os propósitos para os quais foram designadas.
- **Malware:** Software malicioso projetado para infiltrar um sistema computacional com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de software costuma entrar em uma rede por meio de diversas atividades aprovadas pela

empresa, como e-mail ou sites. Entre os exemplos de malware estão os vírus, *worms*, *trojans* (ou cavalos de Troia), *spyware*, *adwareerootkits*.

- **Mídia:** Mecanismos em que dados podem ser armazenados além da forma e da tecnologia utilizada para a comunicação - inclui discos ópticos, magnéticos, CDs, fitas e papel, entre outros. Um recurso multimídia combina sons, imagens e vídeos, que são diferentes tipos de mídia.
- **Nível de acesso:** Especificam quanto de cada recurso ou sistema o usuário pode utilizar.
- **Operador De Dados Pessoais ou Colaborador-Operador:** Pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador.
- **Plano de gerenciamento de incidentes:** Plano de ação claramente definido e documentado, para ser usado em caso de incidente que basicamente englobe os principais recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes.
- **Política de Privacidade e Proteção de Dados Pessoais da H&P:** Política corporativa da Herkenhoff & Prates responsável por estabelecer diretrizes e responsabilidades da H&P que assegurem e reforcem seu compromisso com o cumprimento das legislações de proteção de dados pessoais aplicáveis, em especial, com a Lei Geral de Proteção de Dados ("LGPD", Lei Federal nº 13.709/2018 e alteração promovida pela Lei Federal nº 13.853/2019). Descreve também, as regras gerais a serem seguidas na condução de atividades e operações de tratamento de dados pessoais realizadas pela H&P e pelos destinatários desta Política, no âmbito de suas atividades.
- **Privacidade incorporada aos processos ou *Privacy by design e Privacy by Default*:** Procedimento que visa garantir a privacidade e a proteção de dados pessoais em todas as atividades da H&P, desde a concepção de suas iniciativas e projetos, seu desenvolvimento e/ou na atualização de novos produtos, serviços, processos, práticas de negócio ou sistemas.
- **Quebra de segurança:** Ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação.

- **Segurança da informação:** Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.
- **Senhas:** São um meio comum de validação da identidade do usuário para obtenção de acesso a um sistema de informação, serviço ou dispositivo/mídia (telefone corporativo, notebook, mídias, máquinas fotográficas etc.).
- **Terceiro:** É toda pessoa física ou jurídica contratada pela H&P para desenvolver ou auxiliar no desenvolvimento de suas atividades, tanto na qualidade de fornecedores de bens ou serviços, como de parceiros comerciais.
- **Tratamento de dados pessoais (Tratamento)**: Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle da informação, modificação, comunicação, transferência, difusão ou extração.
- **Uso compartilhado de dados:** Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.
- **Usuários**: São todos os colaboradores que possuem acesso à rede, sistemas e recursos informacionais, disponíveis pela Herkenhoff & Prates.
- **Vírus:** Seção oculta e autorreplicante de um software de computador, geralmente utilizando lógica maliciosa, que se propaga pela infecção (isto é, inserindo uma cópia sua e se tornando parte) de outro programa. Não pode se auto executar, ou seja, necessita que o seu programa hospedeiro seja executado para que se tornar ativo.
- **Vulnerabilidade:** Conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou por uma organização, os quais podem ser evitados por uma ação interna de segurança da informação.

TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE

Declaro que recebi e tive o conhecimento de todo o conteúdo das Política de Segurança da Informação da H&P e Política de Privacidade e Proteção de Dados Pessoais da H&P.

- ✓ Concordo e estou ciente que:
  - Somente posso usar as informações confidenciais ou que contenham dados pessoais ou dados pessoais sensíveis recebidos da H&P com o propósito restrito de se fazer cumprir o estabelecido e acordado no contrato de trabalho, sendo vedada a divulgação a terceiros.
  - Exceto quando imprescindíveis ao desenvolvimento das ações da H&P e integre as suas atividades, não é permitido, ao receber informação confidencial ou dados pessoais e/ou dados pessoais sensíveis, produzir cópias ou *backup*, por qualquer meio ou forma, de quaisquer documentos ou base de dados.
- ✓ Me obrigo, ao receber qualquer informação confidencial ou que contenha dados pessoais e/ou dados pessoais sensíveis a:
  - Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor dessas informações ou dados, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao seu objeto, comprometendo-me a adotar cautelas e precauções adequadas no sentido de impedir o seu uso indevido por qualquer pessoa que, por qualquer razão, tenha tido acesso a elas;
  - Ser responsável por impedir, por qualquer meio em direito admitido, a divulgação ou a utilização de informações ou dados.
- ✓ Estou ciente que, ao receber informação confidencial ou dados pessoais e/ou dados pessoais sensíveis, que as obrigações de confidencialidade e sigilo, tanto quanto as outras responsabilidades e obrigações, vigorarão durante e após todo o contrato de trabalho, mesmo após meu desligamento da empresa.
- ✓ Tenho conhecimento e aceito que, na hipótese de violação de quaisquer dos tópicos mencionados acima, estarei sujeito as medidas administrativas disciplinares e penalidades legais, em especial a prevista no art. 482, da Consolidação das Leis do Trabalho, que trata da rescisão do contrato de trabalho por justa causa, sem prejuízo das perdas e danos que der causa, estas estimadas pela empresa, inclusive as de ordem moral ou concorrencial, bem como as de responsabilidades civil e criminal respectivas.
- ✓ Manifesto minha concordância com todos os termos aqui dispostos, por meio da minha assinatura, reconhecendo a importância dessas regras para a segurança da informação e da própria organização e comprometo-me a cumpri-las integralmente.

Data: .....

Local: .....

Nome: .....

Cargo: .....

Assinatura: .....