

Hubert		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

ÍNDICE

1. OBJETIVO DA POLÍTICA DE SEGURANÇA.....	2
2. COMPROMISSO DA HUBERT E ADMINISTRAÇÃO.....	2
3. COMUNICAÇÃO DA POLÍTICA.....	3
4. PRINCÍPIOS DA POLÍTICA DE SEGURANÇA DE INFORMAÇÃO.	3
5. DESTINATÁRIOS.....	4
6. TREINAMENTO E CAPACITAÇÃO.....	4
7. DESCUMPRIMENTO DA POLÍTICA DE SEGURANÇA.	4
8. RESPONSABILIDADES E COMPETÊNCIAS PELA POLÍTICA	5
8.1. SOBRE A ADMINISTRAÇÃO:	5
8.2. SOBRE A DIRETORIA EXECUTIVA DE TECNOLOGIA:	5
8.3. SOBRE OS GESTORES DE PESSOAS/PROCESSOS (DEPARTAMENTOS/GERÊNCIAS):	6
8.4. SOBRE O COMITÊ DE SEGURANÇA DA INFORMAÇÃO.	6
9. DÚVIDAS E QUESTÕES.	7
10. DENÚNCIAS. INCIDENTES DE SEGURANÇA. USO EM NÃO-CONFORMIDADE. AMEAÇAS. SUSPEITAS.	7
11. RESPONSABILIDADES E COMPETÊNCIAS ESPECÍFICAS DA ÁREA DE TECNOLOGIA DE INFORMAÇÃO:	8
12. POLÍTICA DE USO ACEITÁVEL DOS ATIVOS DA HUBERT	9
12.1. Diretrizes sobre o uso do Correio Eletrônico.....	10
12.2. Diretrizes sobre o uso da Internet	11
12.3. Diretrizes sobre uso de Computadores e Recursos Tecnológicos.....	11
12.4. Diretrizes sobre o uso de Dispositivos Móveis.....	13
13. DIRETRIZES DE MESA E TELA LIMPA.....	14
14. SOBRE OS FORNECEDORES.....	14
15. INFORMAÇÕES CONFIDENCIAIS. OBRIGAÇÃO DE CONFIDENCIALIDADE	15
16. RESPEITO PELA PROPRIEDADE INTELECTUAL DE TERCEIROS.	15
17. DADOS PESSOAIS.....	16

ELABORAÇÃO	REVISÃO	APROVAÇÃO	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
<i>Ulisses Diniz Santos</i>	<i>Dimas Alves</i>	<i>Rodrigo / Daniel</i>	
SETOR: TI	SETOR: TI	SETOR: Diretoria	
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

Hubert		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

18. IDENTIFICAÇÃO E GESTÃO DE ACESSO.....	16
19. INSTALAÇÕES FÍSICAS. DATACENTER.....	16
19.1. SOBRE AS INSTALAÇÕES (INCLUINDO DATACENTER FÍSICO)	16
19.2. SOBRE O DATACENTER CLOUD.....	17
20. POLÍTICA DE GESTÃO DE SOFTWARE	17
21. BACKUP	18
22. ANEXOS	18
23. REFERÊNCIAS	19
24. HISTÓRICO DE REVISÕES	20
25. ARQUIVO DOS DOCUMENTOS.....	20
26. Anexo 01 – Termo de Recebimento da Política.....	21
27. Anexo 02 – Termo de Uso de Equipamento da Hubert.....	22

1. OBJETIVO DA POLÍTICA DE SEGURANÇA.

A presente Política de Segurança de Informação (“Politica”) destina-se a:


Estabelecer processos, práticas e diretrizes que permitam aos seus destinatários, incluindo, mas não se limitando, colaboradores, clientes, prestadores de serviços e fornecedores da Hubert seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo. Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

A presente Política poderá ser revista e atualizada, sempre que necessário ou conveniente, a critério único da Hubert. A revisão e atualização da Política ocorrerá, no mínimo, de forma anual.

2. COMPROMISSO DA HUBERT E ADMINISTRAÇÃO.

A Hubert, por meio da sua administração e gerência, vem por meio desta Política demonstrar seu compromisso e responsabilidade de salvaguardar e proteger os ativos da organização de quaisquer acidentes ou ameaças, incluindo

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

dados e informações de sua propriedade ou sob a sua guarda, tais como seus clientes e fornecedores, nos termos desta Política, e garantir, assim, a continuidade dos negócios.

A presente Política será válida e eficaz a partir da sua publicação, salvo se determinado em contrário.

Nesse sentido, a Hubert compromete-se a:

- (a) Identificar, analisar, monitorar e tratar eventuais riscos e ameaças de segurança a Ativos da Hubert (conforme definição abaixo), por meio de avaliações regulares, periódicas e contínuas;
- (b) Implementar e fiscalizar medidas de segurança e proteção necessárias, adequadas e apropriadas, destinadas a impedir eventuais danos e prejuízos à Hubert, decorrentes da violação do disposto nesta Política, incluindo uso indevido, incidentes ou ataques;
- (c) Disseminar, capacitar e sensibilizar todos os Destinatários (conforme definição abaixo) desta Política sobre a necessidade e relevância da segurança da informação para a prossecução das atividades e negócios da Hubert;
- (d) Promover as atividades, recursos e investimentos necessários para assegurar o cumprimento desta Política.

3. COMUNICAÇÃO DA POLÍTICA.

Ainda, esta Política será devidamente divulgada e disponibilizada a todos os Destinatários (conforme abaixo definido), mediante a utilização de meios, formatos e suportes adequados e apropriados, que permitam seu acesso e consulta a qualquer momento, tais como, por e-mail, via intranet, comunicação presencial, entre outros.

4. PRINCÍPIOS DA POLÍTICA DE SEGURANÇA DE INFORMAÇÃO.

Preservar as informações da Hubert para a consecução dos seus negócios e atividades, e assegurar um relacionamento adequado e transparente com seus clientes, colaboradores e fornecedores, quanto à:

- **Integridade:** garantia de que a informação e dados mantidos pela Hubert, de sua propriedade ou sob sua guarda, sejam devidamente preservados em seu estado original, visando protegê-las, na guarda ou transmissão, e livres e isentos de quaisquer alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** garantia que o acesso à informação somente será realizado por pessoas autorizadas.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

Hubert		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

5. DESTINATÁRIOS.

A presente política é aplicável a todos os usuários e terceiros que tenham acesso a Ativos e Sistemas da Hubert (conforme definição abaixo), ou que venham a acessar as instalações de propriedade ou controladas pela Hubert, incluindo, mas não se limitando, administradores, diretores, executivos, gerentes, empregados, prestadores de serviços, estagiários e fornecedores. Os Destinatários deverão observar, a todo o tempo, o disposto nesta Política, sob pena de aplicação das respectivas sanções e penalidades.

Sem prejuízo do demais dispostos nesta Política, no caso de encerramento de atividades e serviços pelos Destinatários, serão revogados os direitos de acesso dos Destinatários aos Ativos e Sistemas da Hubert.

6. TREINAMENTO E CAPACITAÇÃO.

Todos os Destinatários devem ser conscientizados sobre assuntos envolvendo segurança da informação, por meio da capacitação e treinamento sobre a diversidade de ameaças existentes, medidas de proteção adequadas e apropriadas e a necessidade de denunciar e reportar eventuais incidentes, ameaças, suspeitas, tentativas ou indícios de uso dos Ativos (conforme definição abaixo) em não conformidade com esta Política, destinados a garantir uma utilização adequada e apropriada e não comprometer a segurança da Hubert.

Ainda, deverá ser fornecido um resumo adequado e apropriado desta Política para ser formalmente entregue, aceite e assinado antes do início de qualquer atividade na Hubert.

Os treinamentos e capacitações serão realizados de forma regular e periódica.

7. DESCUMPRIMENTO DA POLÍTICA DE SEGURANÇA.

O descumprimento do disposto na presente Política implicará na aplicação de sanções e penalidades adequadas e apropriadas, conforme o caso aplicável. As sanções serão sempre proporcionais e adequadas à natureza e gravidade do descumprimento.

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

Hubert		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

8. RESPONSABILIDADES E COMPETÊNCIAS PELA POLÍTICA

8.1. SOBRE A ADMINISTRAÇÃO:

- Garantir a disseminação do disposto nesta Política aos Destinatários, inclusive, por meio de suas diretorias e gerências da Hubert;
- Assegurar o cumprimento efetivo desta Política pelos Destinatários;
- Aprovar eventuais alterações e atualizações à Política submetidas pela Diretoria Executiva de Tecnologia;
- Determinar e implementar comitê destinado a assegurar o cumprimento pontual e integral desta Política;
- Disponibilizar recursos e investimentos necessários para assegurar e garantir o cumprimento e atualização desta Política.

8.2. SOBRE A DIRETORIA EXECUTIVA DE TECNOLOGIA:

- Assegurar o cumprimento dos requisitos, medidas e providências que se façam necessárias, adequadas e apropriadas para garantir o cumprimento do disposto nesta Política pelos Destinatários, inclusive, por meio das diretorias, gerências da Hubert;
- Monitorar e fiscalizar o cumprimento efetivo e integral desta Política pelos Destinatários, de forma regular, periódica e contínua;
- Disseminar a cultura de segurança de informação na Hubert, nos termos desta Política, por meio de capacitação e treinamento dos Destinatários (conforme definição abaixo), tais como campanhas e palestras;
- Propor revisões, melhorias e atualizações que se façam necessárias e convenientes desta Política;
- Fornecer as informações e esclarecimentos que venham a ser solicitados pela Administração ou Destinatários que sejam de suas atribuições e competências;
- Processar e apurar eventuais denúncias de ameaças e não-conformidades dos Destinatários com o disposto nesta Política, por meio da realização das investigações que se façam necessárias ou convenientes;
- Processar eventuais incidentes de segurança que venham a ocorrer para assegurar a continuidade de negócios e atividades da Hubert;
- Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação;
- Manter a Administração e Comitê de Segurança devidamente informados sobre assuntos relacionados ao tema que afetem ou tenham potencial para prejudicar à Hubert.

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

Hubert		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

8.3. SOBRE OS GESTORES DE PESSOAS/PROCESSOS (DEPARTAMENTOS/GERÊNCIAS):

- Disseminar a cultura e compromisso da Hubert em relação à segurança da informação, servindo como modelo de conduta para os Destinatários sob a sua gestão e responsabilidade;
- Assegurar aos Destinatários, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade pelo cumprimento desta Política;
- Exigir dos Destinatários a assinatura de quaisquer documentos e termos que se façam necessários para assegurar o cumprimento integral e efetivo desta Política, antes do início de atividades;
- Informar o Departamento de Tecnologia sobre as atividades dos Destinatários, incluindo os Ativos e Informações Confidenciais que estes deverão ter acesso para o cumprimento de suas obrigações, deveres e responsabilidades, para uma avaliação de eventuais riscos e implementação das medidas de segurança adequadas e apropriadas, nos termos desta Política;
- Adequar as normas, os processos, procedimentos e sistemas internos sob sua responsabilidade para atender a esta Política;
- Permitir e assegurar a participação de seus colaboradores em treinamentos e capacitações que venham a ser realizadas.

8.4. SOBRE O COMITÊ DE SEGURANÇA DA INFORMAÇÃO.

Deve ser formalmente constituído por colaboradores com nível hierárquico mínimo de gerência, composto por colaborador de cada uma das seguintes áreas: Diretoria e Tecnologia da Informação.

- Propor investimentos e recursos necessários para assegurar o cumprimento e atualização desta Política, incluindo contratação de fornecedores;
- Avaliar políticas, medidas e providências que se façam necessárias e adequadas para garantir o cumprimento desta Política;
- Analisar medidas e propostas envolvendo eventuais incidentes de segurança, incluindo ameaças ou tentativas, descumprimento desta Política pelos Destinatários, em particular, fornecedores, e propor ações mitigadoras e corretivas;
- Estabelecer processos envolvendo a generalidade das áreas, departamentos e gerências da Hubert, tal como, requisitos para o treinamento e capacitação dos Destinatários no onboarding e à data encerramento de atividades, plano de continuidade de negócio, condições para teletrabalho (incluindo requisitos de segurança aplicáveis a fornecedores);

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

Hubert		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

O Comitê deverá reunir-se com a periodicidade mínima de uma vez a cada seis meses, podendo se reunir de forma extraordinária sempre que necessário ou conveniente.

9. DÚVIDAS E QUESTÕES.

Eventuais dúvidas ou esclarecimentos que se façam necessários ou convenientes sobre a presente Política, deverão ser encaminhadas para: comite_sgi@hubert.com.br.

10. DENÚNCIAS. INCIDENTES DE SEGURANÇA. USO EM NÃO-CONFORMIDADE. AMEAÇAS. SUSPEITAS.

Os Destinatários (conforme definição abaixo) são encorajados a reportarem, de boa-fé, todas e quaisquer situações, eventos, ocorrências ou comportamentos que possam constituir eventuais incidentes de segurança, ameaças, ou utilizações em não-conformidade com o disposto na presente Política, incluindo meras suspeitas ou tentativas. As comunicações deverão ser realizadas por meios dos seguintes canais: comite_sgi@hubert.com.br.

Os Destinatários deverão fornecer o maior número de informações possíveis, tais como, a identidade, práticas e condutas, data da ocorrência, demais participantes, entre outras informações consideradas relevantes. Será protegida a identidade de qualquer pessoa que faça uma denúncia.

Os Destinatários (conforme definição abaixo) não devem realizar, por conta própria, quaisquer tipos de apurações ou investigações.

A apuração ocorrerá de forma sigilosa e confidencial. O denunciante não deve discutir o caso, fatos, suspeitas ou alegações com qualquer terceiro.

A Hubert poderá, por conta própria ou mediante contratação de terceiro, apurar, investigar e examinar eventuais fatos e informações não descritos na denúncia realizada.

Considerando a natureza e gravidade das denúncias, incluindo respectivos indícios e evidências apuradas, a Hubert poderá proceder à sua devida comunicação às autoridades competentes ou terceiros com quem possui relacionamento.

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação


Hubert		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

11. RESPONSABILIDADES E COMPETÊNCIAS ESPECÍFICAS DA ÁREA DE TECNOLOGIA DE INFORMAÇÃO:

Sem prejuízo do demais disposto nesta Política, a Área de Tecnologia de Informação será responsável por:

- Monitorar, testar e fiscalizar a eficácia dos controles utilizados e informar os gestores de eventuais riscos, ameaças, ocorrências, incidentes, incluindo tentativas ou suspeitas, e utilização dos Ativos pelos Destinatários;
- Configurar os Ativos para assegurar a sua conformidade com o disposto nesta Política;
- Segregar as funções administrativas, operacionais e gerenciais a fim de restringir ao mínimo necessário os poderes e prerrogativas, e assim assegurar a proteção e segurança dos Ativos da Hubert;
- Gerar e armazenar registros e trilhas para auditoria com nível de detalhe suficiente para rastrear eventuais riscos, ameaças, ocorrências, incidentes, incluindo tentativas ou suspeitas, e utilização dos Ativos pelos Destinatários. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências;
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Hubert;
- Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela. O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-los? antes que a informação seja definitivamente descartada;
- Garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário, no caso de movimentação interna dos ativos de TI;
- Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que: (i) os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário; (ii) os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante;
- Planejar, implantar, fornecer, monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio;
- Proteger continuamente todos os Ativos contra eventuais ameaças, riscos, incidentes, incluindo tentativas ou suspeitas, e utilização em não conformidade dos Ativos;
- Realizar auditorias periódicas de configurações técnicas e análise de riscos;
- Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

- Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, risco, ameaça, incidente, incluindo tentativas ou suspeitas, uso em não conformidade, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os Ativos ou à Hubert;
- Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro;
- Monitorar o ambiente de TI, gerando indicadores e históricos de:
 - uso da capacidade instalada da rede e dos equipamentos;
 - Logs de execuções de backup;
 - tempo de resposta no acesso à internet e aos sistemas críticos da Hubert;
 - períodos de indisponibilidade no acesso à internet e aos sistemas críticos da Hubert;
 - incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante) ;
 - atividade de todos os colaboradores durante os acessos às redes externas, inclusive via internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

12. POLÍTICA DE USO ACEITÁVEL DOS ATIVOS DA HUBERT


Para a prossecução e execução das atividades, deveres e funções, a Hubert poderá disponibilizar determinados bens, materiais, equipamentos, ferramentas e serviços (“Ativos”) aos Destinatários, incluindo, celular, cartões de acesso, smartphone, arquivos, aplicações, sistemas, notebook, tablet, computador, e-mail e internet. Os Ativos constituem ferramentas de trabalho de propriedade ou sob o controle da Hubert.

Os Ativos serão objeto de inventário, de forma regular e periódica, sendo fornecidos em regime de comodato. Os Destinatários comprometem-se a zelar pela sua guarda, correto manuseio e manutenção em adequado e normal estado de conservação.

Os Destinatários zelarão pela segurança, integridade e utilização adequadas desses Ativos, devendo ser imediatamente comunicado qualquer incidente, evento, ocorrência, furto, ou até mesmo suspeita, envolvendo os Ativos.

Os Ativos deverão ser sempre utilizados, preferencialmente, para finalidades profissionais. A Hubert tem o direito de monitorar, rastrear e fiscalizar a utilização desses Ativos para assegurar sua utilização em conformidade com esta Política.

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

Os Destinatários não gozam de qualquer expectativa de privacidade relativamente à sua utilização. É permitida a utilização razoável dos Ativos para fins pessoais, na medida em que não interfira ou comprometa com o cumprimento dos deveres e responsabilidades profissionais dos Destinatários.

Quaisquer dados de finalidade pessoal, salvo em Ativos de propriedade da Hubert ou qualquer outro armazenamento corporativo, poderão ser apagados sem qualquer aviso prévio, estes dados também não serão inseridos nas rotinas de backup e tão menos serão disponibilizados ao colaborador na devolução do Ativo, independente do motivo da devolução.

Os Ativos deverão ser devolvidos nas condições em que foram disponibilizados (ressalvado o desgaste usual e normal), após a conclusão de suas atividades, deveres e funções, ou mediante solicitação da Hubert. Não é permitida a instalação de qualquer programa, aplicação ou serviço, sem a autorização prévia e expressa da Hubert.

Sem prejuízo do demais disposto nesta Política, é estritamente proibida a utilização dos Ativos para: (i) acessar, visualizar, transmitir, divulgar ou armazenar conteúdos de cunho ou natureza ofensiva, abusivo, indecente, sexual, ilícita, inapropriada, obscena, difamatória ou discriminatória; (ii) violar direitos de terceiros, em especial, o direito de privacidade ou de propriedade intelectual; (iii) praticar qualquer ato contrário à legislação aplicável; (iv) explorar vulnerabilidades, sobrecarregar, prejudicar ou comprometer o funcionamento e desempenho de recursos, equipamentos, sistemas e aplicações de propriedade ou sob controle da Hubert; e (v) realizar atividades remuneradas paralelas. A violação das diretrizes estabelecidas nesta Política poderá ensejar a aplicação de sanções.


12.1. Diretrizes sobre o uso do Correio Eletrônico

As diretrizes sobre o uso de Correio Eletrônico foram separadas para facilitar a manutenção/atualização, evitando verificação de toda esta política a cada necessidade de mudança.

Os Destinatários das diretrizes são todos os setores da Hubert e terão acesso às áreas de Recursos Humanos, tecnologia da Informação e Diretoria da Hubert.

As diretrizes têm a seguinte descrição e deve acompanhar este documento. “Política de Segurança da Informação – Diretriz Uso Correio Eletrônico e Internet”

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

12.2. Diretrizes sobre o uso da Internet

As diretrizes sobre o uso da Internet foram separadas para facilitar a manutenção/atualização, evitando verificação de toda esta política a cada necessidade de mudança.

Os Destinatários das diretrizes são todos os setores da Hubert e terão acesso às áreas de Recursos Humanos, tecnologia da Informação e Diretoria da Hubert.

As diretrizes têm a seguinte descrição e deve acompanhar este documento. “Política de Segurança da Informação – Diretriz Uso Correio Eletrônico e Internet”

12.3. Diretrizes sobre uso de Computadores e Recursos Tecnológicos

Os Destinatários deverão cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis;

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico do Departamento de Tecnologia da Informação da Hubert, ou de quem este determinar. As gerências que necessitarem fazer testes, deverão solicitá-los previamente ao Departamento de Tecnologia da Informação;

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor;

Os sistemas e computadores devem ter versões do software antivírus instalados, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado no service desk enviando e-mail para tecnologia@hubert.com.br;

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário;

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

Hubert		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

Arquivos pessoais e/ou não pertinentes ao negócio da Hubert (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para o Sharepoint, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente sem comunicação prévia ao usuário;

Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos no Sharepoint. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário;

Os colaboradores da Hubert e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização do Departamento de Tecnologia da Informação;

No uso dos computadores, equipamentos e recursos de informática, devem ser observadas as seguintes regras:

- Todos os computadores de uso individual deverão ter senha de Bios para restringir o acesso de colaboradores não autorizados. Tais senhas serão definidas pelo Departamento de Tecnologia da Informação, no qual eles terão acesso para manutenção dos equipamentos;
- Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador;
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico do Departamento de Tecnologia da Informação da Hubert ou por terceiros devidamente contratados para o serviço;
- Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização dos gestores das áreas e da área de informática;
- O colaborador deverá manter a configuração do equipamento disponibilizado pela Hubert, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações;
- Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados;

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

Hubert		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

- Todos os recursos tecnológicos adquiridos pela Hubert devem ter imediatamente suas senhas padrões (default) alteradas;
- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso;

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da Hubert;

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
- Burlar quaisquer sistemas de segurança;
- Acessar informações confidenciais sem explícita autorização do proprietário;
- Vigar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

12.4. Diretrizes sobre o uso de Dispositivos Móveis

A Hubert deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite que eles usem equipamentos portáteis. A concessão se tais dispositivos não enseja o pagamento de quaisquer valores adicionais.

O suporte técnico aos dispositivos móveis de propriedade ou sob o controle da Hubert e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.

Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

Hubert		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico do Departamento de Tecnologia da Informação. O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico do Departamento de Tecnologia da Informação da Hubert.

É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes, desde que sejam respeitadas as regras da diretriz anexas de uso de internet.

Equipamentos portáteis, como smartphones, tablet, Ipad, pen drives e players de qualquer espécie, quando não fornecidos ao colaborador pela instituição, não serão validados para uso e conexão em sua rede corporativa.

13. DIRETRIZES DE MESA E TELA LIMPA

As diretrizes de Mesa e Tela Limpa foram separadas para facilitar a manutenção/atualização, evitando verificação de toda esta política a cada necessidade de mudança.

Os Destinatários das diretrizes são todos os setores da Hubert e terão acesso às áreas de Recursos Humanos e Diretoria da Hubert.

As diretrizes têm a seguinte descrição e deve acompanhar este documento. “Política de Segurança da Informação – Diretriz Mesa e Tela Limpa”

14. SOBRE OS FORNECEDORES

Todos os fornecedores que venham a ter acesso a sistemas de informações relevantes da Hubert, devem ter ciência e concordar, por escrito, com os termos desta Política, antes de ser concedido qualquer acesso. Será disponibilizado um resumo desta Política, ou requisitos de segurança, devendo ser parte integrante do termo, instrumento ou contrato que venha a ser firmado com o referido fornecedor, de forma a garantir a sua conformidade a todo o tempo. Os requisitos de segurança exigíveis dos fornecedores poderão variar de acordo com a essencialidade, relevância e criticidade dos sistemas ou Ativos.

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

Hubert		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

Ainda, não são permitidos o acesso e utilização de Informações Confidenciais da Hubert (conforme definição abaixo) por fornecedores sem a assinatura de termo válido e específico contendo obrigações claras e expressas de sigilo e confidencialidade aplicáveis a esses terceiros.

Todos os contratos com fornecedores serão objeto de monitoramento e fiscalização para garantir que os requisitos de segurança da informação sejam atendidos. Ainda, os contratos devem incluir disposições que permitam o monitoramento e fiscalização pela Hubert, encerramento de atividades no caso de descumprimento desta Política, suspeita ou indícios de incidente de segurança ou risco, bem como garantir o acesso, armazenamento e transferência de informações e dados no caso de encerramento.

15. INFORMAÇÕES CONFIDENCIAIS. OBRIGAÇÃO DE CONFIDENCIALIDADE.

No exercício de suas atividades, os Destinatários poderão ter acesso às informações, dados e documentos de natureza sigilosa e de propriedade ou sob o controle e guarda da Hubert (“Informações Confidenciais”). Não é permitida a utilização, exploração, transmissão, compartilhamento de Informações Confidenciais da Hubert, a qualquer título, em benefício próprio ou de terceiros, com intuito comercial ou não, sem as necessárias garantias, autorizações e licenças.

A seu critério único, a Hubert poderá limitar o acesso e utilização de Informações Confidenciais para garantir a aplicação e cumprimento desta Política. É proibida a utilização de Informações Confidenciais para finalidade distinta daquela para a qual foram autorizadas pela Hubert.

As informações e dados de propriedade ou sob a guarda da Hubert serão armazenados e retidos em local seguro e por prazo adequado e apropriado, considerando a natureza, essencialidade e seu fundamento, e nos termos do permitido pela legislação aplicável.

A transmissão de Informações Confidenciais será objeto de medidas de segurança adequadas e apropriadas.

16. RESPEITO PELA PROPRIEDADE INTELECTUAL DE TERCEIROS.

A Hubert está comprometida e respeita as informações confidenciais e propriedade intelectual de terceiros.

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

Hubert		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

Nesse sentido, e durante suas atividades, os Destinatários poderão ter acesso a informações e dados de natureza sigilosa, confidencial e de propriedade de terceiros, tais como, clientes e fornecedores da Hubert. Os Destinatários deverão guardar sigilo e confidencialidade da propriedade intelectual de terceiros, não podendo ser utilizadas, divulgadas ou transmitidas, em benefício da Hubert ou qualquer outra pessoa.

17. DADOS PESSOAIS.

A Hubert procede ao tratamento de dados pessoais de acordo e em estrita conformidade com sua política de tratamento de dados pessoais e legislação aplicável, possuindo política própria, autônoma e específica sobre o assunto.

18. IDENTIFICAÇÃO E GESTÃO DE ACESSO

As diretrizes de Identificação e Gestão de Acesso foram separadas para facilitar a manutenção/atualização, evitando verificação de toda esta política a cada necessidade de mudança.

Os Destinatários das diretrizes são a área de Tecnologia da Informação (TI), Recursos Humanos e Diretoria, tendo acesso todas os setores da Hubert.

As diretrizes têm a seguinte descrição e deve acompanhar este documento. “Política de Segurança da Informação – Diretriz Identificação e Gestão de Acesso”

19. INSTALAÇÕES FÍSICAS. DATACENTER

19.1. SOBRE AS INSTALAÇÕES (INCLUINDO DATACENTER FÍSICO)

Áreas e espaços que contenham informações, dados sensíveis e relevantes para a Hubert serão de restrito acesso e sujeitos a medidas de segurança e proteção físicas adequadas e apropriadas

O acesso ao Datacenter somente é permitido a colaboradores do Departamento de Tecnologia da Informação, e caso necessário acesso a terceiros para reparos, manutenção devendo ser realizados com acompanhamento de um colaborador da tecnologia da informação.

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

Hubert		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

A limpeza do Datacenter terá que ser acompanhada por uma pessoa do Setor de Tecnologia Informação.

O acesso de visitantes, terceiros ou outros colaboradores do própria Hubert somente poderá ser realizado com acompanhamento de um colaborador autorizado,

O acesso ao Datacenter é por meio de chave digital, e apenas poderá ocorrer em situações de extrema necessidade ou emergência, quando a segurança física do Datacenter for comprometida, como por incêndio, inundação, abalo da estrutura predial, ...

Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização via E-mail com 3 dias de antecedência, encaminhar E-mail para tecnologia@hubert.com.br.

O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Serviços Gerais.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

No caso de desligamento de empregados ou colaboradores que possuam acesso ao Datacenter, imediatamente deverá ser removido seu acesso.

19.2. SOBRE O DATACENTER CLOUD

O acesso aos servidores virtuais hospedados em cloud privada ou pública tem restrição de acesso somente aos administradores de rede e equipe de Tecnologia da Informação. O acesso deve ser realizado através de usuário e senha e com duplo fator de autenticação.

20. POLÍTICA DE GESTÃO DE SOFTWARE

A aquisição ou implementação de software novo ou atualizado, incluindo desenvolvimentos, serão cuidadosamente controlados, planejados, gerenciados e testados pela Hubert. Os riscos de segurança da informação associados a tais projetos serão mitigados por meio de uma combinação de controles técnicos e de procedimentos.

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

Hubert		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

Os requisitos de negócios para a aquisição, implementação e desenvolvimento de novo software ou seus melhoramentos devem levar em consideração e especificar os requisitos para controles de segurança da informação.

Ainda, eventuais desenvolvimentos só entrarão no ambiente de produção após a realização de testes e confirmação de estarem livres de quaisquer códigos maliciosos e/ou indesejado. Serão implementados processos de auditoria do código-fonte e deverão ser incluídas disposições em contratos destinados ao controle e responsabilização de terceiros desenvolvedores. A instalação de software e hardware em ambiente de produção estará sujeito a determinadas regras e formalidades, a serem implementadas, de acordo com a sua relevância, essencialidade e criticidade.

21. BACKUP

Todos os sistemas de informação, dados de natureza corporativa possuem rotinas seguras de backup, sendo devidamente armazenados em cofres de segurança.

Por questões de segurança demais informações referentes à backup estão descritas na diretriz de backup, esta somente terá acesso os membros da diretoria e gestão da tecnologia da informação.

As diretrizes de backup foram separadas para facilitar a manutenção/atualização, evitando verificação de toda esta política a cada necessidade de mudança.

Os Destinatários das diretrizes são a área de Tecnologia da Informação (TI), tendo acesso as áreas da Diretoria, TI e fornecedores que gerenciam e acompanham esta diretriz específica.

As diretrizes têm a seguinte descrição e deve acompanhar este documento. “Política de Segurança da Informação - Diretriz de Backup”.

22. ANEXOS

Os Anexos fazem parte integrante desta Política. Em caso de conflito entre o disposto no Anexo e Política, prevalecerá o disposto nesta Política. Em tudo o que não estiver especialmente disposto na Política, serão aplicáveis os termos e condições do Anexo.

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

Hubert		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

23. REFERÊNCIAS

Katsikas, S.; Gritzalis, D., eds. (1996). Information Systems Security: De frente para a Sociedade da Informação do século 21. IFIP Avanços em Tecnologia da Informação e Comunicação. Springer. P. 358. ISBN 9780412781209 . O modelo McCumber tem grandes semelhanças com o CobiT - Objetivos de Controle para ele - quadro (CobiT 1995).

"Welcome to the ISACA / F". ISACA 18 de outubro de 1996. Arquivado a partir do original em 7 de novembro de 1996. Retirado 24 de junho de 2021.

Luellig, G.; Frazier, J. (2013). "Uma Abordagem COBIT para conformidade regulamentar e Eliminação defensável". ISACA Journal. 5. Retirado 24 de junho de 2021.

Haes, SD;"Capítulo 5: COBIT como um Framework para Governança Corporativa de TI". Governança corporativa de Tecnologia da Informação: Alcançar Alinhamento e Valor, Com COBIT 5 (2ª ed.). Springer. Pp. 103-128. ISBN 9783319145471 . Retirado 24 de junho de 2021.

Stroud, RE (2012). "Introdução ao COBIT 5" (PDF). ISACA. Retirado 24 de junho de 2016.

Da Cruz, M. (2006). "10: AS 8015-2005 - Norma Australiana para Governança Corporativa das TIC". Em van Bon, J.; Verheijen, T. modelos de gestão de TI. Publicação de Van Haren.Pp. 95-102. ISBN 9789077212905 . Retirado 23 de junho de 2021.

"ISO / IEC DIS 29382: 2007 Edition, 01 de fevereiro de 2007". IHS Standards Store. IHS, Inc. arquivados a partir do original em 23 de Junho de 2021. Retirado 23 de junho de 2021.

"ISACA lança COBIT 5: Actualização Quadro para a Governança e Gestão de TI" (PDF). Provitivi, Inc. 18 de maio de 2012. Retirado 24 de junho de 2021.

"COBIT 5 para Segurança da Informação". ISACA. Retirado 24 de junho de 2021.

"COBIT 5 para Assurance". ISACA. Retirado 24 de junho de 2021.

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

Hubert		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

24. HISTÓRICO DE REVISÕES

Nº DA REVISÃO	DATA	ITEM ALTERADO	DESCRIÇÃO DA ALTERAÇÃO	RESPONSÁVEL PELA ALTERAÇÃO	JUSTIFICATIVA
01	09/12/2021	Não se aplica	Não se aplica	Ulisses Santos	Elaboração Inicial

25. ARQUIVO DOS DOCUMENTOS

REGISTRO	LOCAL DE ARQUIVO	RESPONSÁVEL DO ARQUIVO	FORMA DE ARQUIVO	PERÍODO DE RETENÇÃO

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

Hubert		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

26. Anexo 01 – Termo de Recebimento da Política

Anexo 01 – Termo de Recebimento da Política de Segurança da Informação

Declaro, para todos os fins, o recebimento de exemplar de Política de Segurança da Informação da Hubert, e desde já concordo e reconheço ser essencial observar, respeitar e cumprir, de forma integral e pontual, o disposto nesta Política, para proteger e salvaguardar os seus negócios, atividades e clientes.

Ainda, estou ciente que o eventual descumprimento de qualquer uma das disposições constantes desta Política poderá causar danos e prejuízos sérios e irreparáveis financeiros e não-financeiros à Hubert, incluindo, à sua reputação, imagem e prestígio no mercado e junto a clientes.

O seu descumprimento poderá acarretar a aplicação de determinadas sanções e penalidades de natureza proporcional à gravidade da ocorrência.

Nesse sentido, declaro, nesta data, ter ciência e estar de acordo com os procedimentos acima descritos, comprometendo-me a respeitá-los e cumpri-los plena e integralmente.

De acordo e aceite:

São Paulo, _____, de _____, de _____.

(nome do colaborador)

(Gerente de RH / Matrícula / CPF)

Este documento deve ser assinado em 02 (duas) vias.

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

Hubert		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021


27. Anexo 02 – Termo de Uso de Equipamento da Hubert

O Termo de Uso de Equipamentos foi separado para facilitar a manutenção/atualização, evitando verificação de toda esta política a cada necessidade de mudança.

O Destinatário deste termo é a área de Tecnologia da Informação (TI), tendo acesso as áreas da Diretoria, TI, Recursos Humanos e todos os colaboradores que utilizam equipamentos de propriedade da Hubert.

O termo tem a seguinte descrição e deve acompanhar este documento. “Política de Segurança da Informação Hubert – Anexo02”.

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO DIRETRIZ DE IDENTIFICAÇÃO DE ACESSO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

A presente Diretriz de Identificação e Gestão de Acesso (“Diretriz”) faz parte integrante da Política de Segurança de Informação da HUBERT (“Política”). Esta Diretriz poderá ser revista e atualizada sempre que necessário ou conveniente, a critério único da Hubert,

Em caso de conflito entre o disposto nesta Diretriz e Política, prevalecerão as disposições da Política.

IDENTIFICAÇÃO E GESTÃO DE ACESSO

SOBRE A IDENTIFICAÇÃO

Todos os usuários devem ter um identificador único (ID do usuário) para seu uso pessoal e exclusivo para acesso a todos os Ativos da Hubert. O ID do usuário não deve ser usado por ninguém e as senhas associadas não devem ser compartilhadas com qualquer outra pessoa, salvo motivo justificativo atendível.

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a Hubert e/ou terceiros.

Todos os dispositivos de identificação utilizados na Hubert, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados, assinaturas digitais e os dados biométricos devem estar associados a uma pessoa física somente, e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário é responsável pelo uso correto dos Ativos perante a Hubert e demais terceiros, nos termos da legislação aplicável.


É proibido o compartilhamento de login e acessos de Ativos da Hubert.

O Departamento de Tecnologia da Informação responde pela criação da identidade lógica dos colaboradores na instituição, conforme solicitado no formulário de checklist do Novo Colaborador e de acordo com o Fluxo de Abertura de Vagas RH.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

Serão implementados controles de acesso para todos os Ativos de forma a garantir a segurança de informação da Hubert.

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO DIRETRIZ DE IDENTIFICAÇÃO DE ACESSO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

SOBRE A GESTÃO DE SENHAS

Os usuários deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais (@ # \$ %) e variação entre caixa alta e caixa baixa (maiúsculo e minúsculo) sempre que possível.

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres alfanuméricos, utilizando caracteres especiais (@ # \$ %) e variação de caixa alta e caixa baixa (maiúsculo e minúsculo) obrigatoriamente, além da dupla autenticação (MFA).

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com Departamento de Tecnologia da Informação da Hubert.

Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

Os usuários podem alterar a própria senha e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é 90 (noventa) dias, não podendo ser repetidas as 3 (três) últimas senhas. Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada 60 dias.

Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.

No caso de encerramento de atividades ou serviços dos Destinatários, tal como, contrato de trabalho ou prestação de serviços, o Departamento de Recursos Humanos / entidade responsável pela contratação do fornecedor comunicará, de imediato, tal fato ao Departamento de Tecnologia da Informação, para o encerramento dos acessos aos Ativos da Hubert e adoção das demais providências necessárias (incluindo devolução de crachás e Ativos, quando aplicável).

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação


Hubert		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO DIRETRIZ DE IDENTIFICAÇÃO DE ACESSO	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou ir pessoalmente à área técnica responsável para cadastrar uma nova.

A diretriz de Identificação e Gestão de Acesso foi fragmentada para facilitar a manutenção/atualização, evitando verificação de toda a política de segurança da Informação, a cada necessidade de mudança.

Esta diretriz destina-se a todos os setores e terão acesso os setores de Recursos Humanos, Tecnologia da Informação e Diretoria da Hubert.

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO DIRETRIZ DE MESA E TELA LIMPA	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

A presente Diretriz de Mesa e Tela Limpa (“Diretriz”) faz parte integrante da Política de Segurança de Informação da HUBERT (“Política”). Esta Diretriz poderá ser revista e atualizada sempre que necessário ou conveniente, a critério único da Hubert.

Em caso de conflito entre o disposto nesta Diretriz e Política, prevalecerão as disposições da Política.


DIRETRIZ DE MESA E TELA LIMPA

Os Destinatários deverão:

- (i) Manter a necessária cautela quando da exibição de dados em tela impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;
- (ii) Não se ausentarem da estação de trabalho sem encerrar a sessão de uso do navegador, bloquear a estação de trabalho, bem como encerrar a sessão do cliente de correio, garantindo assim a impossibilidade de acesso indevido por terceiros;
- (iii) não consumir quaisquer alimentos, bebidas na mesa de trabalho e próximo aos equipamentos;
- (iv) armazenar quaisquer documentos, materiais ou mídias, em especial, contendo Informações Confidenciais, em locais seguros, separados e devidamente trancados sempre que não sejam necessários, em particular, em períodos de ausência e fora do horário de trabalho;
- (v) preservar e proteger documentos, materiais ou mídias, em especial, aqueles que contém Informações Confidenciais, não os mantendo em locais de acesso público ou não reservados.

Esta diretriz destina-se a todos os setores da Hubert e o setor de Recursos Humanos e Diretoria da Hubert terão acesso.

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO DIRETRIZ SOBRE O USO DO CORREIO ELETRÔNICO E INTERNET	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

A presente Diretriz sobre o Uso de Correio Eletrônico e da Internet (“Diretriz”) faz parte integrante da Política de Segurança de Informação da HUBERT (“Política”). Esta Diretriz poderá ser revista e atualizada sempre que necessário ou conveniente, a critério único da Hubert.

Em caso de conflito entre o disposto nesta Diretriz e Política, prevalecerão as disposições da Política.

DIRETRIZES SOBRE O USO DO CORREIO ELETRÔNICO E DA INTERNET

O objetivo desta norma é informar aos colaboradores e prestadores de serviços da Hubert quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico da Hubert é para fins corporativos e relacionados às atividades do usuário dentro da instituição. A utilização desse serviço para fins pessoais não é permitida.

Para que um endereço de e-mail seja criado pelo Setor de Tecnologia da Informação é necessária a solicitação via formulário de Checklist do Novo Colaborador/Prestador de Serviço e um chamado no service desk tecnologia@hubert.com.br, pelo RH e pela liderança imediata do colaborador ou, a depender do caso, pela área contratante, para registro e execução da tarefa em questão.

Para fins de segurança, poderão ser criados correios eletrônicos corporativos para prestadores de serviços, de acordo com as condições contratuais negociadas.


Todas as caixas de e-mail possuem log de acesso, controle de alteração de senha e são factíveis de auditoria sem aviso prévio, desde que devidamente autorizada pela diretoria.

Por questões de segurança pode ser exigido para determinadas caixas de e-mail, o uso de MFA, (Duplo Fator de Autenticação).

É proibido o uso do correio eletrônico da Hubert para:

- enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- enviar mensagem por correio eletrônico pelo endereço de seu departamento, usando o nome de usuário de outra pessoa ou endereço de correio eletrônico não autorizados;

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO DIRETRIZ SOBRE O USO DO CORREIO ELETRÔNICO E INTERNET	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

- enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Hubert ou suas unidades vulneráveis a ações civis ou criminais;
- divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades da Hubert estiver sujeita à algum tipo de investigação.
- produzir, transmitir ou divulgar mensagem que:
 - contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Hubert;
 - contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
 - contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
 - vise obter acesso não autorizado a outro computador, servidor ou rede;
 - vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
 - vise burlar qualquer sistema de segurança;
 - vise vigiar secretamente ou assediar outro usuário;
 - vise acessar informações confidenciais sem explícita autorização do proprietário;
 - vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- tenha conteúdo considerado impróprio, obsceno ou ilegal;
- seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- tenha fins políticos locais ou do país (propaganda política) ;
- inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador/prestador de serviço
- Gerência ou departamento ou área de atuação
- Nome da empresa

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

Hubert		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO DIRETRIZ SOBRE O USO DO CORREIO ELETRÔNICO E INTERNET	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

- Telefone(s)

DIRETRIZES SOBRE O USO DA INTERNET

Se necessário, a Hubert poderá bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação;

A Hubert, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas;

Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor;

A utilização pessoal da internet não deve: comprometer a banda da rede em horários estritamente comerciais; não perturbar o bom andamento dos trabalhos; nem implicar conflitos de interesse com os seus objetivos de negócio;

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet;

Os colaboradores com acesso à internet não poderão fazer o download (baixa) de programas na internet. O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pelo Departamento de Tecnologia da Informação;

Os colaboradores não poderão em hipótese alguma utilizar os recursos da Hubert para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional;

O acesso a sites de entretenimento, vídeos ou músicas poderão ser realizados por usuários que tenham atividades profissionais relacionadas a essas categorias. Para tal, grupos de segurança, cujos integrantes deverão ser definidos pelos respectivos gestores, precisam ser criados a fim de viabilizar esse acesso especial;

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

Hubert		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO DIRETRIZ SOBRE O USO DO CORREIO ELETRÔNICO E INTERNET	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021


Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado a Hubert ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados;

Os colaboradores não poderão utilizar os recursos da Hubert para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores;

O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos, ou outros softwares que possuem o mesmo intuito.

O uso do WhatsApp para fins corporativos deve ser aplicado nos mesmos termos e orientações descritos nesta Política, reiterando que quaisquer informações e arquivos confidenciais e de terceiros, assim que transmitidos/recebidos através do WhatsApp, devem ser armazenados no SharePoint para sua guarda segura. E após isso, apagada do WhatsApp, que não deve ser um meio utilizado para guarda de arquivos e dados de quaisquer origens.

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO ANEXO 02 – TERMO DE USO DE EQUIPAMENTOS DA HUBERT	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

27. Anexo 02 – Termo de Uso de Equipamentos da Hubert

Anexo 02 – Termo de Uso de Equipamentos da Hubert

Nome do Empregado (“Usuário”):

CPF:

Identificação do Equipamento (“Equipamento”): [●]

Ativo no.: [●]

Descrição do ativo:

Marca: [●]

Modelo: [●]

Acessórios: [●]

Outras Características: [●]

O presente Termo de Responsabilidade de Equipamento (“Termo”) destina-se a regular os termos e condições de uso por Usuário (conforme identificado acima) do Equipamento (conforme identificado acima) disponibilizado pela Hubert, os quais são regulados nos termos em que seguem:


(i) O presente Termo faz parte integrante da Política de Segurança de Informação da Hubert (“Política”). Em tudo o que não estiver especialmente disposto aqui, será aplicável à Política. Em caso de conflito entre o disposto neste Termo e a Política, será aplicável à Política;

(ii) O Equipamento destina-se preferencialmente para fins profissionais. É permitida a utilização razoável dos Ativos para fins pessoais, na medida em que não interfira ou comprometa com o cumprimento dos deveres e responsabilidades profissionais do usuário;

(iii) A seu critério único, a Hubert poderá determinar a substituição ou não do Equipamento, definindo, ainda, período de troca, tipo, marca, modelo e acessórios a serem concedidos;

(iv) A presente autorização de uso do Equipamento não é concedida em caráter definitivo, reservando-se a Hubert, a qualquer tempo, o direito de retomar, trocar ou alterar os aparelhos eletrônicos objetos deste Termo de Responsabilidade, descaracterizando-se, assim, qualquer direito ou interpretação diversa daquela aqui mencionada;

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação


		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO ANEXO 02 – TERMO DE USO DE EQUIPAMENTOS DA HUBERT	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

(v) O Usuário declara que recebeu o Equipamento e acessórios em perfeitas condições para o uso, obrigando-se pelas suas manutenções, utilizações e guarda, dentro das especificações técnicas acerca das quais foi cientificado, para a sua devida utilização;

(vi) sem prejuízo do demais disposto neste Termo, o Usuário obriga-se, ainda, a:

- a) Manter o Equipamento em condições de limpeza adequadas;
- b) Operar o Equipamento de acordo com as orientações e diretrizes da Hubert;
- c) Manter o Equipamento em local seguro e adequado;
- d) Não instalar ferramentas, aplicações, sistemas ou acessórios no Equipamento, sem o prévio conhecimento e autorização escrita da Hubert;
- e) Não proceder a nenhuma intervenção técnica com ou sem o uso de ferramentas;
- f) Não ceder, tampouco permitir o uso, ainda que temporário, do Equipamento a terceiros, sob quaisquer pretextos, sem o conhecimento e autorização prévia, por escrito, da Hubert;
- g) Não descarregar, carregar, instalar, executar softwares, programas, arquivos, pastas ou sistemas, incluindo aplicativos, no Equipamento que não tenham licenças de propriedade da Hubert e que não forem autorizados, por escrito;
- h) Utilizar quaisquer aplicativos ou programas de computador em estrita conformidade com as instruções ou especificações de uso fornecidas pela Hubert;
- i) Respeitar as normas do fabricante do Equipamento e as determinações das autoridades competentes relacionadas ao uso do Equipamento;
- j) Utilizar o Equipamento, devendo responder pelos danos e prejuízos causados a ele, bem como àqueles causados a terceiros em decorrência de sua utilização;
- k) Informar prontamente a Hubert, através do e-mail, tecnologia@hubert.com.br ou a quem a Hubert determinar, sobre qualquer falha, dano ou mau funcionamento do Equipamento;
- l) Permitir que a Hubert solicite o Equipamento e acessórios em retorno e/ou efetue vistorias, sempre que a Hubert entender necessário;
- m) Na ocasião em que o Usuário efetuar a devolução do Equipamento e acessórios, ou em qualquer outra averiguação feita pelo departamento de tecnologia, estes serão objeto de vistoria e caso sejam encontradas avarias não decorrentes do seu uso normal, o ocorrido passará por avaliação de comitê de auditoria, que fará uma análise e definirá se haverá sanção ou abono dos prejuízos causados. Havendo sanção será responsabilizado pelos danos constatados, autorizando o desconto dos prejuízos diretamente de sua remuneração, salário (se aplicável) e/ou verbas rescisórias, e se houver abono dos prejuízos, nada será cobrado do usuário;
- n) Não acessar, carregar, descarregar, transmitir, instalar, disponibilizar, compartilhar, armazenar e imprimir páginas ou conteúdos de sítios de internet, redes sociais, redes públicas de internet sem fio, programas de computador,

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO ANEXO 02 – TERMO DE USO DE EQUIPAMENTOS DA HUBERT	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

arquivos, pastas, materiais e informações que, na diligência de um indivíduo prudente, possam ter conteúdos impróprios, ofensivos, ilícitos, censuráveis ou até mesmo introduzir códigos maliciosos no Equipamento;

- o) Manter adequados e atualizados sistemas e medidas de segurança no Equipamento destinados a prevenir e impedir a utilização e o acesso não autorizados por terceiros a arquivos, pastas, correio eletrônico, perfis e contas eletrônicas, tal como mecanismos de identificação, autenticação (contas e senhas de acesso) e autorização;
- p) Não permitir o acesso, divulgação ou transmissão de informações sigilosas e de propriedade da Hubert, ou de terceiros com a qual a Hubert tenha obrigação de confidencialidade, tal como métodos e planos de negócio, designs, especificações, fórmulas, modelos, fluxogramas, contratos, projetos, conceitos de produto;
- q) Não utilizar o Equipamento para a prática de qualquer ato ou procedimento ilícito, ofensivo, impróprio ou censurável, bem como respeitar e não infringir a legislação brasileira aplicável; e
- r) Informar e apresentar Equipamento a Hubert sempre que houver suspeita de que a sua integridade, acesso e segurança se encontram comprometidos ou foi objeto de violação por terceiro (incidente, ameaça, incluindo, tentativa);

Parágrafo Único. Para efeitos da alínea n), entende-se por código malicioso todo e qualquer programa, link, arquivo ou Pastas sem prejuízo de outras modalidades, destinados a explorar as vulnerabilidades do Equipamento, executar ações danosas e não autorizadas, interferir ou comprometer o seu regular uso, incluindo arquivos, e respectivas medidas de proteção, acessar informações confidenciais e de natureza proprietária da Hubert, tal como vírus, worms, bot e botnet, spyware, backdoors, cavalos de tróia e rootkits.

(vii) O Usuário será responsável por qualquer perda ou dano, a que der causa por infração ao presente Termo;

(viii) Caso o Equipamento seja objeto de furto, roubo, extraviado, perdido ou de qualquer forma saia do controle do Usuário, este deverá efetuar, sempre que aplicável, o respectivo boletim de ocorrência nas autoridades competentes e comunicar imediatamente a Hubert, sem prejuízo de outras providências que venham a ser determinadas. Referido procedimento não eximirá o Usuário de reembolsar a Hubert dos danos e prejuízos causados, caso haja uma sanção definida pelo comitê de auditoria dos danos causados;

(ix) Em caso de ocorrência do disposto no (viii) acima ou eventuais danos causados no Equipamento, ou que venham a ser causados a terceiros em razão do Equipamento, o Usuário deverá reembolsar a Hubert pelos danos sofridos, nos termos da legislação aplicável, em caso de sanção, definido pelo comitê de auditoria; sendo aplicável também no caso de uso indevido, incorreto e inadequado do Equipamento pelo Usuário;

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação

Hubert		Política de Segurança da Informação	Política	
Tecnologia da Informação	Revisão: 01	SEGURANÇA DA INFORMAÇÃO ANEXO 02 – TERMO DE USO DE EQUIPAMENTOS DA HUBERT	Módulo: 01	Aprovação: 08/12/2021
			Elaboração: 01/10/2021	Publicação: 09/12/2021

(x) É expressamente proibido ao Usuário ceder, doar, alugar, vender, arrendar, duplicar, emprestar, reproduzir, disponibilizar ou explorar o acesso de terceiros, de forma remota ou não, incorporar a outros programas ou sistemas, próprios ou de terceiros, oferecer em garantia ou penhor, alienar ou transferir, total ou parcialmente, a qualquer título, de forma gratuita ou onerosa, quaisquer programas e/ou aplicativos existentes no Equipamento;

(xi) O Equipamento, incluindo seus acessórios, são de propriedade da Hubert e intransferíveis, sendo que, em caso de rescisão de contrato ou afastamento de qualquer natureza sofrido, todos os itens disponibilizados deverão ser devolvidos imediatamente à Hubert, na forma em que foram entregues, ressalvado o desgaste usual decorrente do seu uso normal e regular;

(xii) O Usuário não goza de presunção de privacidade na utilização dos equipamentos da Hubert, que poderá, de tempos em tempo, monitorar os equipamentos;

(xiii) Todas as disposições e responsabilidades assumidas pelo Usuário neste Termo, permanecerão vigentes durante todo o período de uso do Equipamento, bem como durante o período de apuração e conclusão de eventuais danos ocorridos durante a posse dos aparelhos pelo Usuário.

De acordo e aceite:

São Paulo, _____, de _____, de _____.

(Nome do colaborador)

Gerente de RH / Matrícula / CPF)

Este documento deve ser assinado em 02 (duas) vias.

ELABORAÇÃO <i>Ulisses Diniz Santos</i> SETOR: TI	REVISÃO <i>Dimas Alves</i> SETOR: TI	APROVAÇÃO <i>Rodrigo / Daniel</i> SETOR: Diretoria	ESCLARECIMENTOS E SUGESTÕES CONTACTAR
RUBRICA	RUBRICA	RUBRICA	SETOR: Tecnologia da Informação