Tipo / Type:	Política / Policy
Nome / Name:	Gestão de Risco de Informação por Partes Externas / External Party Information Risk Management
Nível / Level:	Standard Bank Angola / Standard Bank Angola
Classificação / Classification:	Pública (Controlada) / Public (Controlled)
Proprietário / Owner:	Departamento de Risco Não-Financeiro e Responsável de Privacidade de Dados/ Non-Financial Risk Department and Data Privacy
Comité de Governação / Governance committee	Comité de Gestão de Risco / Risk Management Committee
Aprovado por / Approved by:	Comité de Risco do Conselho de Administração / Board Risk Committee
Data de Aprovação / Approval Date:	22-Novembro-2022 / 22-November-2022
Data de Efectividade / Effective Date:	22-Novembro-2022 / 22-November-2022
Data da próxima revisão / Next review Date	22-Novembro-2023 / 22-November-2023
Contacto / Contact:	claudia.lima@standardbank.co.ao

Classificação

Este documento foi emitido estritamente para efeitos empresariais internos do Standard Bank Angola e suas subsidiárias

Classification

This document has been issued strictly for business purposes of Standard Bank Angola and its Third Parties, their subsidiaries and business associates

Gestão de Risco de Informação por Partes Externas	*External Party Information Risk Management*
1. DECLARAÇÃO DA POLÍTICA	**1. POLICY STATEMENT**
1.1 O Standard Bank Angola (o Banco) estabeleceu objectivos estratégicos de alto nível para mostrar o compromisso do Banco de implementar boas práticas de gestão de riscos de informação e segurança de informação.	1.1 The Standard Bank (the Bank) has established high level policy objectives to show the Bank's commitment to implement good information risk management and information security practices.
1.2 O Risco de Informação é definido como o risco de uso, modificação, divulgação ou destruição de activos de informação, acidentais ou intencionais, que compromete a confidencialidade, integridade e disponibilidade de informações e que prejudicaria potencialmente o negócio.	1.2 Information Risk is defined as the risk of accidental or intentional unauthorized use, modification, disclosure or destruction of information assets, which would compromise the confidentiality, integrity and availability of information and which would potentially harm the business.
1.3 O Banco conta com partes externas e seus funcionários (Terceiro ou Terceiros) para prestar serviços ao Banco, para prestar serviços em nome do Banco ou fornecer produtos. Em todos os casos, esses Terceiros, sejam pessoas físicas ou jurídicas, têm acesso a informação do Banco e activos de informação do Banco para fins de contratação e fornecimento desses serviços e produtos.	1.3 The Bank relies on external parties and their personnel (Third Party or Third Parties) to deliver services to the Bank, to deliver services on behalf of the Bank or supply products. In all instances these Third Parties, whether individuals or corporate entities, have access to Bank information and Bank information assets for the purpose of contracting and delivering these services and products.
1.4 Esta política estabelece os requisitos para o uso aceitável dos activos de informação do Banco (incluindo informação electrónica, física e audível) por Terceiros que prestam serviços ou produtos ao Banco.	1.4 This policy establishes the requirements for acceptable use of the Bank information assets (including electronic, physical, video and audible information) by Third Parties providing services or products to the Bank.
1.5 Estes activos de informação são para uso comercial dos utilizadores autorizados do Banco. Os dispositivos e a media física do Banco, e os dados e informações de propriedade armazenados neles permanecem, sempre, propriedade do Banco.	1.5 These information assets are for the business use of the Bank's authorised users. The Bank's devices and physical media, and the proprietary data and information stored on them remain at all times, the property of the Bank.
1.6 Os Terceiros devem ser cuidadosos ao transmitir, comunicar ou depositar qualquer informação do Banco, para evitar divulgação a pessoas ou entidades não autorizadas. Devem ser seguidos os controlos adequados para salvaguardar a confidencialidade da informação do Banco.	1.6 Third Parties must take care whenever transmitting, communicating, or relaying any Bank information, to prevent disclosure to unauthorized persons or entities. Appropriate controls must be followed to safeguard the confidentiality and integrity of the Bank's information.
1.7 Os funcionários de terceiros, funcionários temporários e subcontratados com acesso aos activos de informação do Banco devem ler esta política e assinar os documentos relevantes de reconhecimento de políticas (ver secção relevante desta política ou acordo relevante com o Banco). Estes documentos com assinatura devem ser mantidos por Terceiros e, quando entregues, tanto pelo Banco como pelo Terceiro.	1.7 Third Party employees, temporary employees, contractors and sub-contractors with access to Bank information assets must read this policy and sign the relevant policy acknowledgement documents (see relevant section of this policy or relevant agreement with the Bank). These signoff documents must be retained by the Third Party and the Bank.

2. APLICABILIDADE	2. APLICABILITY
2.1 Esta política aplica-se a todos os Terceiros, seus funcionários e subcontratados, incluindo "recursos não permanentes" com as seguintes categorias:	2.1 This policy applies to all Third Parties, their personnel and sub-contractors including "non-permanent resources" with the following categories:
a. Funcionário com Contrato a Tempo Determinado, que tem ou pode ter meios de acesso aos activos de informação do Banco.	a. Limited Term Employee, Independent Contractor, Labour Broker Resource and Turnkey, who has or may have the means of access to Bank information assets.
b. Terceiros provedores de serviços (por exemplo, prestadores de serviços na nuvem, provedor de centro de dados, desenvolvedores de software, provedor de centro de chamadas, provedor de armazenamento físico, etc.), que são a entidade que executa a actividade terceirizada (por exemplo, computação em nuvem, ambiente local, armazenamento de sites, etc.) em nome do Banco, como entidade regulada.	c. Third party service providers (e.g. cloud service provider, data centre hosting provider, software developers, call centre provider, physical storage provider, etc.), who are the entity that executes the outsourced (e.g. cloud computing, hosted environment, off-site storage, etc.) activity on behalf of the Bank, as a regulated entity.
d. Os Terceiros que prestam serviços aos seus clientes usando a infraestrutura e os sistemas do Banco com ou sem que os clientes do terceiro estejam cientes do envolvimento do Banco (por exemplo, concessionárias de automóveis, comerciantes, credores de títulos, etc).	e. Third Parties that deliver services to its customers using Bank infrastructure and systems with or without the customers of the third party being aware of the involvement of the Bank (e.g. car dealerships, merchants, bond originators, etc.).
2.1 Esta política aplica-se a ambos os dados (a representação de factos como texto, números, gráficos, imagens, som ou vídeo); e informações (dados em contexto) no formato audível (falado em conversação), físico e electrónico (incluindo a propriedade intelectual do Banco) de propriedade ou confiadas ao Banco ao longo do ciclo de vida da informação, incluindo informação em movimento, informação em uso e informação em repouso.	2.2 This policy applies to both data (the representation of facts as text, numbers, graphics, images, sound or video); and information (data in context) in audible (spoken in conversation), physical and electronic format (including the Bank's intellectual property) owned by or entrusted to the Bank throughout the information lifecycle, including information in motion, information in use and information at rest.
3. REQUISITOS MÍNIMOS DE CONFORMIDADE COM ESTA POLÍTITA	**3. MINIMUM REQUIREMENTS TO COMPLY WITH THIS POLICY**
3.1 Princípios	3.1 Principles
Os seguintes princípios devem ser de adesão obrigatória por parte de Terceiros e orientar a implementação dos requisitos mínimos conforme estabelecido nesta Política:	Third Parties must adhere to the following principles. The principles prescribe the implementation of the minimum requirements, by the Third Party, as set out in this Policy:
a. Proteger a confidencialidade (propriedade da informação secreta ou privada dentro de um grupo predeterminado), integridade (propriedade da informação de alta qualidade, válida, precisa, não sendo adulterada nem representada incorretamente) e disponibilidade	a. Protecting the confidentiality (property of information being secret or private within a predetermined Bank), integrity (property of information being high quality, valid, accurate, not being tampered with nor incorrectly represented) and availability (property of

(propriedade da informação acessível e utilizável quando necessário) da informação.	information being accessible and useable when required) of information.
b. A informação é um activo valioso para o Banco e deve ser protegida.	b. Information is a valuable asset to the Bank and must be protected.
c. Todos os formatos de informação, impressos, audíveis ou electrónicos, estruturados ou não estruturados, devem ser protegidos.	c. All formats of information, hardcopy, audible or electronic, structured or unstructured, must be protected.
d. Proteger a informação ao longo do seu ciclo de vida, que consiste em Originar (ou seja, criar, receber ou adquirir), Usar (ou seja, processar ou transmitir), Reter (isto é, armazenar, fazer backup ou arquivar) e Eliminar (ou seja, destruir ou transferir).	d. Protect information throughout its lifecycle, which consists of Originate (i.e. create, receive or acquire), Use (i.e. process or transmit), Retain (i.e. store, back-up or archive) and Dispose (i.e. destroy or transfer).
e. Proteger a informação independentemente da sua localização (por exemplo, centros de dados, instalações locais, locais remotos ou terceirizados, dispositivos de propriedade pessoal).	e. Safeguard the information regardless of its location (e.g. owned data centres, hosted premises, remote or outsourced sites, personally owned devices).
f. Proteger a tecnologia ou o dispositivo no qual a informação é hospedada para garantir que a informação armazenada também esteja protegida.	f. Protect the technology or device on which the information is hosted to ensure that the stored information therein is also protected.
g. Certificar-se do não repúdio (a capacidade de provar que uma acção ou evento ocorreu e não pode ser negado mais tarde) da informação.	g. Ensure the non-repudiation (the ability to prove an action or event has taken place and cannot be denied later) of information.
h. A propriedade e a responsabilidade devem ser garantidas para proteger os activos de informação de ameaças potenciais (fonte potencial de um evento com probabilidade de ocorrência) que possam explorar vulnerabilidades (fraqueza num sistema de informação, procedimentos, controlos internos, implementação ou organização).	h. Ownership and accountability must be taken for protecting information assets from potential threats (potential source of an event with a likelihood of occurrence) that may exploit vulnerabilities (weakness in an information system, procedures, internal controls, implementation or organisation).
i. São necessárias medições e relatórios apropriados, qualitativos e quantitativos	i. Appropriate qualitative and quantitative measurements and reporting is required.
j. Seguir uma abordagem padrão de privacidade desde o início para garantir que o processamento da informação dê efeito ao direito a privacidade	j. Follow a privacy-by-design by default approach to ensure processing of information gives effect to the right to privacy.
3.2 Gestão de Relações	3.2 Relationship Management
a. Um ponto de contacto claro dentro do Banco (por exemplo, superior hierárquico relevante ou gestor de projeto) e do Terceiro (por exemplo, gestor de conta de cliente ou	a. A clear contact point between the Bank (e.g., relevant line manager or project manager) and the Third Party (e.g. client account manager or project manager) must be

gestor de projeto) devem ser autorizados e mantidos para lidar com consultas e comunicação.	maintained to handle enquiries and communication.
3.3 Gestão de risco/segurança de informação	3.3 Information risk/security management
a. A Parte Terceira deve ter em vigor (quando aplicável e quando aceitável para o Banco) um universo adequado de risco de informação ou política de segurança e universo de normas, que no mínimo:	a. The Third Party must have in place (where applicable and as acceptable to the Bank) an appropriate and adequate information risk or security policy and standards universe, which at a minimum:
i. Tem o apoio, aprovação e envolvimento activo da gestão senior.	i. Has the support, approval and active engagement of its senior management.
ii. É periodicamente, ou quando há mudanças significativas na Parte Terceira que afectam o risco de informação, analisado, mantido e aprovado.	ii. Is periodically, or when there are significant changes at the Third Party that impact information risk, reviewed, maintained and approved.
b. A Parte Terceira deve:	b. The Third Party must:
i. Ser responsável pela implementação e manutenção da gestão do risco/segurança da informação e gestão de privacidade.	i. Have assigned the responsibility for implementing and maintaining information risk/security and privacy management.
ii. Quando relevante para o Banco, incluir no contrato dos colaboradores e subcontratados, funções e responsabilidades de gestão de risco/segurança da informação e comunicar isso aos seus empregados e subcontratados.	ii. Where relevant to the Bank, include in its employees and sub-contractor contracts, information risk / security and privacy management roles & responsibilities and communicate this to its employees and sub-contractors.
iii. A Parte Terceira deve ter organizado um plano de respostas cibernético, providenciar ao Banco tal plano e participar nas simulações de resposta (onde aplicável).	iii. The Third Party must have in place a Cyber response plan, provide such plan to the Bank and participate in response simulations (where applicable).
3.4 Gestão do Activo de Informação	3.4 Information Asset Management
a. Certificar-se que, para todos os activos de informação do Banco, na posse do Terceiro, os proprietários de informações são identificados e documentados.	a. Ensure that for all Bank information assets, in the possession of the Third Party, the Bank information owners are identified and documented.
b. Os Terceiros devem classificar a informação do Banco de acordo ao nível do seu valor, sensibilidade e criticidade, bem como requisitos legais, regulamentares e de negócio. O esquema de classificação de segurança de informação do Banco deve ser usada como referência.	b. Third Parties must classify Bank information in a manner relative to the level of its value, sensitivity, criticality as well as legal, regulatory and business requirements. The Bank information security classification scheme must be used as reference.
c. Os activos sensíveis de informação física do Banco só podem ser retirados das instalações ou zona física controlada do Banco, com a autorização prévia da pessoa	c. Sensitive physical Bank information assets may only be taken outside of Bank controlled physical location or zone, with the prior

mandatada para autorizar a remoção de activos de informação.	authorisation from the person mandated to authorise removal of information asset.
d. Deve-se ter cuidado para garantir que informações confidenciais não sejam divulgadas em público, por meio de comunicação audível, comunicação electrónica não garantida ou por meio de media física sem a devida autorização.	d. Care must be taken to ensure that sensitive and confidential information is not disclosed in public, via audible communication, unsecured electronic communication or by physical media without proper authorisation.
e. Documentos físicos (ex. impressos) que contenham informações confidenciais devem ser removidos imediatamente da máquina (impressora multifuncional, etc.) depois de terem sido transmitido, recebidos ou impressos para proteger a confidencialidade das informações.	e. Hardcopy (e.g. printed) documents that contain sensitive information must be removed immediately from the machine (multifunction printer, etc.) after having been transmitted, received or printed to protect the confidentiality of the information.
f. Ao enviar por fax um documento contendo informações confidenciais, o destinatário deve primeiro ser contactado e solicitado a estar presente para receber a mensagem de fax.	f. When faxing a document containing sensitive information, the recipient must first be contacted and requested to be present for the receipt of the fax message.
g. Os Terceiros devem devolver activos de informação do Banco no término ou mudança de emprego, contrato ou acordo. A devolução dos activos de informação do Banco deve ser realizado antes do último dia de emprego/contrato ou mais cedo em caso de rescisão sumária.	g. Third Parties must return Bank information assets on termination or change of their employment, contract or agreement, unless specifically provided for in the contract or agreement. Return of the Bank information assets must be conducted prior to the last day of employment/contract or sooner in the event of summary termination.
h. A Parte Terceira deve ter procedimentos e políticas para garantir que os activos de informação do Banco sejam tratados de forma segura, desde a recepção até o final da relação com o Banco.	h. The Third Party must have procedures and policies in place to ensure that the Bank information assets are securely handled, from receipt to the end of the relationship with the Bank.
i. Os processos e procedimentos de Terceiros devem garantir que os activos de informação do Banco sejam adequadamente copiados e arquivados ou eliminados conforme acordado com o Banco.	i. Processes and procedures of the Third Party must ensure that the Bank information assets are appropriately backed-up and archived or disposed of as agreed with the Bank.
3.5 Segurança de Capital Humano	3.5 Human Resources Security
a. Antes da Contratação	a. Prior to Employment
i. As funções e responsabilidades de segurança da informação dos funcionários de Terceiros, trabalhadores temporários e subcontratados com acesso aos activos de informação do Banco devem ser claramente definidas, documentadas e formalizadas nos contratos.	i. Information security roles and responsibilities of the Third-Party employees, temporary employees, contractors and sub-contractors with access to the Bank information assets must be clearly defined, documented, and formalised in the contracts.

ii. Devem ser efectuadas verificações de antecedentes e de referência a colaboradores de Partes Terceiras, trabalhadores temporários e subcontratados antes do início de actividades laboral relativos ao Banco. Quando necessário, o Banco irá rever e decidir se as verificações são suficientes para atender aos padrões de verificação do Banco.	ii. Background and reference checks must be performed on Third Party employees, temporary employees, contractors and sub-contractors before commencement of work relating to the Bank. Where necessary the Bank will review and decide if the checks are sufficient to meet the vetting standards of the Bank.
iii. O rastreamento de segurança e a verificação de funcionários relevantes de Terceiros, trabalhadores temporários e subcontratados devem ser realizados antes do início do trabalho para o qual foi contratado de acordo com a função que a pessoa irá desempenhar.	iii. Security screening and vetting of relevant Third-Party employees, temporary employees, contractors and sub-contractors must be carried out before commencement of the contracted work in accordance with the role the person will be fulfilling.
b. Durante vigência do Contrato	b. During Employment
i. A gestão de Terceiros deve assegurar que os funcionários, contratados e subcontratados com acesso aos activos de informação do Banco confirmem periodicamente que leram, releram e cumprirão as políticas e procedimentos de segurança estabelecidos pelos Terceiros, para proteção dos activos de informação do Banco.	i. Third Party management must ensure employees, contractors and sub-contractors with access to the Bank information assets periodically confirm that they have read, re-read and will comply with the applicable Third Party established security policies and procedures for the protection of the Bank information assets.
ii. A reavaliação de funcionários, temporários ou subcontratados de Terceiros deve ser realizada durante o contrato, se exigido pelo Banco.	ii. Re-screening or re-assessment of employees, temporary employees or subcontractors of Third Party must be carried out during the contract if required by the Bank.
iii. Deve haver um processo disciplinar formal que seja aplicado nos casos em que funcionários, trabalhadores temporários ou subcontratados de Terceiros tenham cometido falhas de segurança envolvendo activos de informações do Banco e/ou os requisitos desta política.	iii. There must be a formal disciplinary process in place that is applied in instances where employees, temporary employees or sub-contractors of the Third Party have committed breaches of security involving Bank information assets and/or the requirements of this policy.
c. Alteração ou Rescisão do Contrato	c. Change or Termination of Employment
i. O acesso aos activos de Informação do Banco deve ser revogado imediatamente após a rescisão do contrato, ou alterado no caso de mudança de função, aviso prévio ou disciplinar de qualquer funcionário, trabalhador temporário ou subcontratado da Parte Terceira.	i. Access to Bank Information assets must be revoked immediately upon termination of employment or contract or amended in the event of a change of role, notice period or disciplinary matter of any employee, temporary employees, contractors or sub-contractor of the Third Party.
3.6 Controlo de Acesso	3.6 Access control

a. O acesso aos activos de informação do Banco deve ser restrito apenas a pessoas autorizadas.	a. Access to Bank information assets must be restricted to authorised individuals only.
b. Os indivíduos e os sistemas que acedem aos activos de informação do Banco devem ser identificados de forma exclusiva e medidas de autenticação apropriadas usadas para autenticar as suas identidades antes do acesso (por exemplo, identificação, senha, autenticação multi-factor, biometria, etc.).	b. Individuals and systems accessing Bank information assets must be uniquely identified and the appropriate authentication measures used to authenticate their identity prior to access (e.g. ID tag, password, multi-factor authentication, biometrics, etc.).
c. A partilha de contas (nome da conta, número ou identificador pessoal) é proibida.	c. Sharing of accounts (personal identifiable account name, number or identifier) is prohibited.
d. Deve haver um processo seguro e consistente de provisionamento de acesso (*on-board*) para criar contas de utilizadores, emitir credenciais de utilizadores e conceder direitos de acesso com base na função da pessoa.	d. There must be a secure and consistent access provisioning (on-boarding) process for creating user accounts, issuing user credentials and granting access rights based on the role of an individual.
e. Os direitos de acesso serão concedidos com o princípio do "privilégio mínimo" e "necessidade de saber" em mente e relativo a função que a pessoa está a desempenhar.	e. Access rights will be granted with the principles of "least privilege" and "need to know" in mind and relative to the role the person will be fulfilling.
f. Os direitos de acesso serão periodicamente analisados para garantir que apenas funcionários activos e autorizados continuam a ter acesso aos activos de informação do Banco.	f. Access rights will be periodically reviewed to ensure that only active and authorised individuals still have access to the Bank information assets.
g. A ParteTerceira deve garantir que há propriedade e responsabilidade na gestão de controlos de acesso para seus funcionários e subcontratados ao longo do seu ciclo de vida.	g. The Third Party must ensure that there is ownership and accountability for the management of access controls for Third Party employees, contractors and subcontractors through its life-cycle.
h. As contas de utilizadores com acesso aos activos de informação do Banco devem ter nomes exclusivos que são directamente atribuíveis a uma única pessoa.	h. User accounts with access to the Bank information assets must have unique names that are directly attributable to a single individual.
i. Todas as contas de utilizadores, identificadores, funções de acesso e privilégios devem ser compilados numa lista, com manutenção regular, que detalha o(s) nível(s) de acesso e identidade de cada pessoa.	i. All the user accounts, identifiers, access roles and privileges must be compiled in a maintained list which details each individual's access level(s) and identity
j. O acesso aos activos informação do Banco devem ser suspensos se não forem utilizados por sessenta ou mais dias consecutivos.	j. Access to the Bank information assets must be suspended if not used for sixty or more consecutive days.
k. Os acessos aos activos de informação do Banco que não são utilizados por noventa dias devem ser desactivados.	k. Access to the Bank information assets that is not used for ninety days must be disabled.

l. Os funcionários, utilizadores temporários e subcontratados de Terceiros que acedem aos activos de informação do Banco remotamente, devem ser autenticados usando pelo menos mecanismos de autenticação de dois factores.	l. Employees, temporary users and sub-contractor users of the Third Party accessing the Bank information assets remotely must be authenticated using at least two-factor authentication mechanisms.
m. Os superiores hierárquicos e responsáveis pela informação de Terceiros devem rever anualmente as contas de utilizadores e os privilégios de acesso para lidar com os activos de informação do Banco e garantir que apenas usuários relevantes tenham acesso autorizado de acordo com as suas funções, aos activos de informação.	m. Line managers and Information owners of the Third Party must annually review user accounts and access privileges for handling the Bank information assets to ensure only relevant users have authorised role-based access to Bank information assets.
n. O acesso de Terceiros aos activos de informação do Banco deve ser analisado e alterado pela gestão quando há uma mudança na função, e deve ser removido após a rescisão do contrato.	n. Third Party access to Bank information assets must be reviewed and changed by management when there is a change in job role and must be removed on termination of their employment or contractual agreement.
o. As credenciais de autenticação (por exemplo, senhas) NUNCA devem ser divulgadas. Se um indivíduo ou Terceiro suspeitar que a confidencialidade das suas credenciais de autenticação tenha sido comprometida, os mesmos devem mudá-la imediatamente e informar o representante do Banco designado.	o. Authentication credentials (e.g. passwords) must NEVER be disclosed to anyone. If an individual or Third-Party suspect that the confidentiality of their authentication credentials has been compromised, they must change it immediately and inform the agreed designated Bank representative.
p. As senhas são o mecanismo de autenticação de acesso lógico mínimo necessário:	p. Passwords are the minimum required logical access authentication mechanism:
i. A complexidade e duração da senha devem ser adequados e proporcionais ao risco associado as infracções e aos activos de informação a serem protegidos.	i. Password strengths and durations must be appropriate and proportionate to the risk associated with breaches and the information assets to be protected.
ii. As senhas não devem ser escritas a menos que sejam protegidas de outra forma, por exemplo, usando criptografia aprovada pelo Banco e armazenadas.	ii. Passwords may not be written down unless protected in some or other form e.g. by using Bank approved encryption and locking it away.
q. Controlos de acesso físicos apropriados devem ser implementados.	q. Appropriate physical access controls must be implemented.
r. A autenticação multifactor deve ser habilitada para sistemas de alto risco, informações secretas e utilizadores privilegiados.	r. Multi-factor authentication must be enabled for high-risk systems, secret information and privileged users.
3.7 Gestão de Alterações	3.7 Change Management
a. A gestão de alterações deve ser aplicada aos activos de informação, sejam eles elementos de informação propriamente ditos ou os sistemas e processos relacionados com a informação, e somente as alterações aprovadas de emergência e/ou formalmente testadas e aceitas devem ser implementadas.	a. Change management must be applied to information assets, whether this be information elements themselves or the systems and processes related to the information and only approved emergency and / or formally tested and accepted changes are to be implemented.

b. A(s) parte(s) relevante(s) do Banco devem ser incluídas como partes interessadas no processo de Gestão de Alterações de Terceiros quando as alterações afectarão o Banco e os seus activs de informação (ex. mudanças no pessoal, mudanças em sistemas, etc.)	b. The relevant part(s) of The Bank must be included as a stakeholder in the Third Party Change Management process when changes will affect the Bank and its information assets (e.g. changes in personnel, changes in systems, etc.)
c. Notificação atempada de alterações de segurança nos activos de Terceiros que suportam o fornecimento de serviços do Banco devem ser fornecidas ao Banco.	c. Timely notification of security changes within Third Party assets supporting the delivery of the Bank's services must be provided to the Bank.
d. Alterações significativas nos controlos físicos e/ou ambientais nas instalações de Terceiros para manusear os activos de informação do Banco devem ser aprovadas pelo Banco.	d. Significant changes to physical and/or environmental controls at the Third-Party sites for handling the Bank information assets must be approved by the Bank.
e. Alterações de subcontratados, outras partes com acesso a informação do Banco ou localização de armazenamento de informação do Banco (por exemplo, *offshoring* e Nuvem) devem ser comunicadas ao Banco. Estas alterações podem estar sujeitas a aprovação prévia do Banco, particularmente quando isso envolve o processamento posterior de informações do Banco ou pode ter um impacto legal e/ou de conformidade regulamentar.	e. Changes of subcontractors, other parties with access to Bank information, or storage location of Bank information (e.g. offshoring and Cloud) must be communicated to the Bank. These changes may be subject to prior approval by the Bank, particularly when it involves further processing of Bank information or may have a legal and/or regulatory compliance impact.
3.8 Privacidade de Dados	3.8 Data Privacy
a. A Parte Terceira deve cumprir com a legislação de proteção de dados (ex. protecção de dados pessoais) e os códigos de conduta aplicáveis no País e em que a informação do Banco possa ser usada ou armazenada pelo Terceiro.	a. The Third Party must comply with data protection legislation and codes of conduct (e.g. protection of personal data) applicable in the country and in which Bank information may be used or stored by the Third Party.
b. A Parte Terceira deve apenas processar informação pessoal de acordo com a obrigação contratual conforme definido no acordo com o Banco e com autorização por escrito do Banco.	b. The Third Party must only process Personal Information in accordance with the contractual obligation as defined in the agreement with the Bank and with written authorisation of the Bank.
c. A Parte Terceira poderá, onde aplicável, colaborar com o Banco no fornecimento de informação necessária concernente a conformidade com a legislação de protecção de dados, código de conduta e obrigações contractuais com o Banco.	c. Where applicable, Third Party will co-operate with the Bank by providing necessary information pertaining to Third Party's compliance with data protection legislation, code of conduct and contractual obligation with the Bank.

d. O aprovisionado desta política será aplicável como requisitos mínimos e pode ser sustentado por uma obrigação contratual em particular entre o Banco e o Terceiro. Se a política contradizer alguma obrigação contratual entre ambas as partes, tais contradições devem ser escaladas ao Responsável de Risco de Informação do Banco para esclarecimento e decisões sobre quais requisitos aplicar-se-á.	d. The provision of this policy will apply as minimum requirements and can be supplemented by particular contractual obligation between Third Party and the Bank. If this policy contradicts with any contractual obligation between parties, such contradiction must be escalated to the Bank Information Risk for clarity and decision as to which requirement will apply.
e. Envio ou partilha de informação do Banco (incluindo informações sobre clientes) com qualquer Terceiro ou, processamento com qualquer outro propósito que não seja o que a parte terceira tem a obrigação de cumprir, nos termos de um acordo com o Banco:	e. Sending or sharing Bank information (including customer information) with any other Third-Party, or processing for purposes other than what the third party is required to do with it in terms of an agreement with the Bank:
i. É proibido quando não autorizado pelo Banco.	i. Is prohibited when not authorised by the Bank.
ii. É permitida apenas quando a informação perde a sua identificação e nunca pode ser associada de volta ao Banco (inclui informações de clientes do Banco).	ii. Is permissible only when the information is de-identified and can never be linked back to the Bank (this is inclusive of Bank customer information).
f. A Parte Terceira deve notificar o Banco da sua intenção de notificar o regulador e concordar com o Banco quando a notificação deve ser efectuada, onde necessário ou onde houver motivos razoáveis para acreditar que as informações pessoais tenham sido acedidas ou adquiridas por partes não autorizadas.	f. The Third Party must notify the Bank of its intention to notify the regulator and agree with the Bank when notification will be done, where necessary or where it has reasonable grounds to believe that Personal information has been accessed or acquired by unauthorised parties.
g. A Parte Terceira deve ter processos internos e externos para notificar os reguladores e obter o consentimento das pessoas afectadas pelo Tratamento de Informações Pessoais, quando necessário; ou onde houver motivos razoáveis para acreditar que a informação pessoal destas pessoas foram acedidas ou adquiridas por partes não autorizadas.	g. The Third Party must have internal and external processes to notify regulators of and obtain consent from affected persons for the Processing of Personal Information, where necessary; or where it has reasonable grounds to believe that Personal Information of such persons has been accessed or acquired by unauthorised parties.
h. Em instâncias onde haja disputa relacionada ao processamento de informação pessoal, a disputa deve ser escalada a gestão de Risco de Informação.	h. In instances where there is a dispute regarding the Processing of Personally Identifiable Information, the dispute must be escalated to Information Risk.

i. O Processamento de Informação Pessoalmente Identificável (incluindo o ciclo de vida da informação) só deve ser efectuado durante o tempo necessário para qual a finalidade da Informação Pessoal foram originalmente recolhidas, ou fornecidas, pelo Terceiro, de acordo com os requisitos de retenção regulamentares, ou desde que legalmente permitido, após o qual a Informação Pessoal deve ser eliminada ou tornada anónima.	i. Processing of Personally Identifiable Information (including the full life-cycle Information) must only be done for as long as it is necessary for the purpose for which the Personally Identifiable Information was originally collected by, or provided to, the Third-Party, in line with legislative retention requirements, or as long as legally permitted, where after the Personal Information must be deleted or rendered anonymous.
3.9 Partilha/Intercâmbio de Informação	3.9 Exchange of Information
a. Os acordos formais devem ser estabelecidos para a troca dos activos de informação do Banco entre o Banco e o Terceiro, e de Terceiros com outras partes aprovadas pelo Banco.	a. Formal agreements must be established for the exchange of the Bank information assets between the Bank and Third-Party, and the Third Party and other Bank approved parties.
b. A Parte Terceira deve ter políticas, procedimentos e controlos técnicos adequados para proteger os activos de informação do Banco partilhados através de qualquer canal de comunicação onde este seja um requisito no âmbito do acordo com o Banco.	b. The Third-Party must have policies, procedures and appropriate technical controls in place to protect the Bank information assets exchanged via any communication channel where this is a requirement in terms of the agreement with the Bank.
3.10 Disponibilidade da Informação	3.10 Availability of Information
a. A Parte Terceira deve implementar medidas para garantir a disponibilidade de activos de informação do Banco em sua posse (por exemplo, backups, soluções de alta disponibilidade, armazenamento redundante, digitalização de documentos físicos ou conforme acordado com o Banco).	a. The Third Party must implement measures to ensure the availability of Bank information assets in its possession (e.g. back-ups, high-availability solutions, redundant storage, digitisation of physical documents, or as agreed with the Bank).
b. A Parte Terceira deve participar nos testes de recuperação de desastres do Banco, onde aplicável.	b. The Third Party must participate in Bank Disaster Recovery tests, where applicable.
3.11 Armazenamento e eliminação de dados em Média	3.11 Media storage and disposal
a. Todos os activos de informação do Banco na posse de Terceiros devem ser armazenados de forma segura em áreas adequadamente seguras, sempre que não estejam em uso.	a. All Bank information assets in the possession of the Third Party must be securely stored in appropriately secure areas whenever not in use
b. Os activos de informação do Banco não devem ser armazenados em suportes de armazenamento portáteis sem o consentimento prévio expresso do Banco.	b. The Bank information assets must not be stored on portable storage media without explicit prior consent from the Bank.
c. Todos os sistemas de terceiros utilizados para processar e armazenar a informação do Banco, devem, quando não forem mais necessários, ser eliminados de forma segura após serem limpos, de forma a evitar a reconstrução da informação do Banco.	c. All Third-Party systems used to process and store the Bank information, must, when they are no longer required, be disposed of securely and safely after being wiped in a manner that would prevent the reconstruction of the Bank information.

d. Todos os activos de informação do Banco devem ser eliminados de forma segura e de tal forma que o activo da informação e os dados contidos nesse activo, caso algum, sejam irrecuperáveis.	d. All information assets of the Bank must be disposed of securely and in such a way that the information asset and the data contained within that asset, if any, is irrecoverable.
3.12 Écran e Secretárias Limpos	3.12 Clear Screen and Clear Desk
a. O écran deve estar sempre bloqueado quando não está em uso.	a. The screen must be locked when devices are not in use.
b. No final de cada dia, ou quando as mesas ou escritórios estão desocupados, qualquer informação interna, confidencial ou secreta do Banco deve ser trancada de forma segura (por exemplo, em armários, gavetas ou gabinetes, que foram fornecidos, conforme apropriado).	b. At the end of each day, or when desks or offices are unoccupied, any Bank internal, confidential or secret information must be locked away securely (e.g. in pedestals, filing cabinets or offices, which have been provided, as appropriate).
c. Todos os resíduos de papel, com informação sensível ou importante para o Banco, devem ser triturados ou colocados nas caixas de trituração seguras localizadas em áreas apropriadas	c. All wastepaper, with any sensitive or information that is important to the Bank, must be shredded or placed in the secure shredding boxes located in appropriate areas.
3.13 Gestão da Vulnerabilidade	3.13 Vulnerability management
a. A Parte Terceira deve garantir que os seus equipamentos informáticos e dispositivos móveis têm patches actualizados aplicados e software de antivírus activado para não infectar os activos de informação do Banco quando estes sistemas e dispositivos de Terceiros tiverem sido autorizados para acesso a sistemas de informação do Banco.	a. The Third Party must ensure that its computer equipment and mobile devices have up to date patches applied and anti-malware software activated so as to not infect the Bank's information assets when these Third-Party systems and devices have been authorised to access Bank information systems.
b. A Parte Terceira deve, se solicitado, permitir que uma avaliação independente seja realizada nos aplicativos que armazenam, processam ou transmitem informação do Banco para identificar e resolver vulnerabilidades técnicas, por ex. teste de penetração, analise de códigos.	b. The Third Party must, if requested, allow for an independent assessment to be conducted on the applications that store, process or transmit Bank information in order to identify and resolve technical vulnerabilities, e.g. penetration-testing, code scans.
3.14 Controlos físicos e ambientais	3.14 Physical and environmental controls
a. Como parte da selecção e diligência de um Terceiro, devem ser fornecidas ao Banco informações para aprovação na segurança das instalações físicas onde os activos de informação do Banco serão acedidos, processados ou armazenados.	a. As part of the selection and due diligence of a Third Party, information must be provided to the Bank for approval on the security of the physical sites where the Bank information assets will be accessed, processed or stored.
b. Caso solicitado, o Terceiro deve autorizar colaboradores do Banco ou consultores que actuem em nome do Banco, a visitar as instalações físico onde os activos de informação do Banco serão processados.	b. If requested, the Third Party must authorise Bank staff or consultants acting on behalf of the Bank, to visit the physical site where the Bank information assets will be processed.

c. Caso solicitado, o Terceiro deve autorizar colaboradores do Banco, ou consultores que actuem em nome do Banco, a avaliar os controlos de segurança das instalações.	c. If requested, the Third Party must authorise the Bank staff, or consultants acting on behalf of the Bank, to assess the site's security controls.
d. Devem existir controlos para garantir que o equipamento utilizado para processar os activos de informação do Banco não podem ser movimentados, removidos, actualizado ou reconfigurados sem autorização formal.	d. Controls must be in place to ensure equipment used to process the Bank information assets cannot be moved, removed, upgraded or reconfigured without formal authorisation.
e. O equipamento usado para processar os activos de informaçãoo do Banco deve ser localizado de forma a proteger contra ameaças ambientais, incluindo, entre outros, incêndio, fumo, água e pó.	e. Equipment used to process Bank information assets must be sited in such a manner to protect against environmental threats, including but not limited to fire, smoke, water and dust
f. O equipamento da Parte Terceira deve estar protegido de forma apropriada contra o acesso não autorizado enquanto estiver a ser reparado por outras pessoas que não Terceiro.	f. The Third-Party's equipment must be appropriately secured from unauthorised access whilst being repaired by persons other than the Third Party itself.
3.15 Gestão de Incidentes	3.15 Incident Management
a. A Parte Terceira deve ter um plano de resposta a incidentes de informação documentado e testado.	a. The Third-Party must have a documented and tested information incident response plan.
b. A Parte Terceira deve imediatamente (ou seja, no prazo de 48 horas) informar potenciais ou reais incidentes de risco de informação a designada função ou representante do Banco, ou conforme acordado entre as partes.	b. The Third Party must immediately (i.e. at the latest within 48 hours) report potential or actual information risk incidents to the designated Bank function or representative, or as agreed in the Third-Party agreement.
c. A Parte Terceira deve cooperar com o Banco durante o processo de gestão de incidentes.	c. The Third Party must cooperate with the Bank during the incident management process.
d. Todos os incidentes de crime financeiro, independentemente do valor monetário, devem ser registrados para que a Unidade de Controlo de Crime Financeiro do Banco possa decidir se deve investigar.	d. All financial crime incidents, no matter what the monetary value, must be recorded so the Bank Financial Crime Control Unit can decide whether they should investigate.
e. Os Incidentes que não têm impacto financeiro directo para o Banco devem ser reportados se reflectirem uma falha num controlo chave ou uma inadequação da estrutura de controlo ou modelo operacional, o que, por sua vez, destaca as lições a serem aprendidas. Se houver alguma dúvida se incidente deve ser reportado, a função de risco operacional do Banco fornecerá orientação caso a caso. As quebras da confidencialidade da informação são sempre reportáveis.	e. Incidents that do not have a direct financial impact to the Bank must be reported if they reflect a failure of a key control, or an inadequacy of the control framework or operating model, which in turn highlights lessons to be learnt. If there is any doubt as to whether an incident must be reported, Bank operational risk functions will give case-by-case guidance. Information confidentiality breaches are always reportable.

f. Os incidentes de risco de informação reportados devem ser registados, avaliados, resolvidos e divulgados com base nos processos e normas de gestão de incidentes do Banco, dentro dos prazos acordados.	f. Reported information risk incidents must be recorded, assessed, resolved and disclosed based on the Bank incident management processes and standards, within agreed timelines.
g. O nível de gravidade do incidente de risco de informação reportado deve ser avaliado - caso necessário, consultando com o Banco - e acções apropriadas implementadas.	g. The severity level of the reported information risk incident must be assessed – where necessary, in consultation with the Bank – and appropriate action taken.
h. Preservar e proteger todas as potenciais provas relacionadas ao incidente e actividades de resposta pelo menos enquanto o Banco exigir que o Terceiro mantenha as provas e de outra forma em termos dos requisitos legais e regulamentares relevantes.	h. All potential evidence related to an incident and response activities must be preserved and protected for at least as long as the Bank requires the Third-Party to retain the evidence and otherwise in terms of the relevant legal and regulatory requirements.
i. Uma analise pós-incidente deve ser realizada e acções correctivas devem ser implementadas para reduzir a probabilidade de recorrência de um incidente de risco de informação.	i. A post-incident review must be conducted, and remedial action must be taken to reduce the likelihood of the information risk incident recurring.
j. A Parte Terceira deve escalar ou interagir com o representante designado do Banco se houver alguma incerteza sobre como lidar com possíveis incidentes de risco de informação.	j. The Third Party must escalate or engage with the designated Bank representative if there is any uncertainty regarding how to handle or deal with potential information risk incidents.
3.16 Investigações	3.16 Investigations
a. A Parte Terceira deve cooperar com o Banco e com todas as partes designadas pelo Banco durante as investigações.	a. The Third-Party must cooperate with the Bank and any parties appointed by the Bank during investigations.
b. A Parte Terceira deve preservar e proteger qualquer informação relacionada com o assunto da investigação, pelo menos, enquanto o Banco exija que o Parte Terceira mantenha as provas e, de outra forma, em termos dos requisitos legais e regulamentares relevantes.	b. The Third-Party must preserve and protect any information related to the subject of the investigation for, at least, as long as the Bank requires the Third Party to retain the evidence and otherwise in terms of the relevant legal and regulatory requirements.
c. A ParteTerceira deve divulgar ao Banco, onde legalmente permitido, se algum dos activos de informação do Banco estiverem envolvidos ou sujeitos a uma investigação.	c. The Third-Party must disclose to the Bank, where legally permissible, if any Bank information assets are involved in or subject to an investigation.
d. Terceiros autorizados a conduzir investigações forenses ou de monitoramento podem não realizar o monitoramento sem a aprovação da(s) pessoa(s) do Banco responsável(s) por Terceiros.	d. Third Parties authorised to conduct forensic investigations or monitoring may not conduct monitoring without an approval from the Bank person(s) responsible for the Third Party.
3.17 Aquisição, desenvolvimento, manutenção e desactivação do sistema	3.17 System acquisition, development, maintenance and retirement

a. Adquirir e desenvolver um novo sistema de TI em nome do Banco ou que terá impacto nos activos de informação do Banco, deve seguir um processo aprovado para avaliar os riscos de informação e definir os controlos de risco e os requisitos de capacidade necessários, com a participação do Banco.	a. Acquiring and developing a new IT system on behalf of the Bank or that will impact on Bank information assets, must follow an approved process to assess the information risks and define the required information risk controls and capacity requirements, with input from the Bank.
b. O cumprimento dos requisitos de risco de informação do Banco (como esta política) devem ser verificados antes de adquirir um novo produto de TI, se este afectar os activos de informação do Banco.	b. Compliance with Bank information risk requirements (such as this policy) must be verified before acquiring a new IT product, where it impacts on Bank information assets.
c. Os dados capturados ou recebidos devem ser validados para garantir o processamento correcto da Informação do Banco.	c. Data captured or received must be validated to ensure correct processing of Bank Information
d. A saída de dados deve ser validada para garantir que o processamento da informação do Banco esteja correcta.	d. Data output must be validated to ensure that the processing of Bank information was correct.
e. O uso de dados de teste deve ser protegido, controlado e não permitido num sistema de produção.	e. The use of test data must be protected, controlled and not allowed in a production system.
f. Se informações do Banco de natureza pessoal, ou de outra forma sensível, são usadas para fins de teste, todos os detalhes e conteúdo sensíveis devem ser removidos ou modificados para além do reconhecimento antes de serem usados.	f. If personal or otherwise sensitive Bank information is used for testing purposes, all sensitive details and content must be removed or modified beyond recognition before use
g. A modificação dos aplicativos fornecidos pelo fornecedor deve ser aprovada pelo Banco, se essas modificações tiverem impacto nos activos de informação do Banco e nos processos de negócios. A modificação deve ser controlada e limitada as mudanças necessárias.	g. Modification to vendor-supplied applications must be approved by the Bank where these modifications will impact on Bank information assets and business processes. Modification must be controlled and limited to necessary changes
h. Os ambientes de produção, desenvolvimento e teste devem ser separados onde a informação do Banco está envolvida.	h. Production, development and testing environments must be segregated where Bank information is involved.
i. A separação de funções para desenvolvedores e usuários de produção deve ser aplicada onde a informação do Banco está envolvida.	i. Segregation of duties for developers and production users must be enforced where Bank information is involved.
j. As abordagens e métodos de desenvolvimento de software seguro devem ser seguidos onde os recursos de informação do Banco estão envolvidos.	j. Secure software development approaches and methods must be followed where Bank information assets are involved.
k. O descomissionamento ou a retirada de um sistema de TI que afecta a informação do Banco e os processos de negócios só devem ocorrer após consulta do Banco e apôs receber a aprovação necessária do Banco.	k. Decommissioning or retirement of an IT system that impacts on Bank information and business processes must only occur after consultation with the Bank and receipt of the necessary approval from the Bank.

l. Os critérios de aceitação (de acordo com os requisitos de risco de informação do Banco e a arquitectura de referência) devem ser estabelecidos, contra os quais devem ser realizados testes adequados (incluindo segurança) para que os defeitos sejam remediados antes de colocar o sistema em produção.	l. Acceptance criteria (in line with Bank information risk requirements and reference architecture) must be established, against which, suitable tests (including security) must be carried out in order for defects to be remediated prior to placing the system in production.
m. Cada sistema de TI adquirido ou desenvolvido deve estar sujeito a um contracto de manutenção e acordo de nível de serviço quando o sistema suportar processos de negócios do Banco.	m. Each acquired or developed IT system must be subject to a maintenance contract and service level agreement when the system supports Bank business processes.
n. Os requisitos para a actividade de manutenção relacionada com o hardware e ao software devem ser especificados e aderidos onde os activos de informação do Banco estão envolvidos.	n. Requirements for maintenance activity relating to hardware and software must be specified and adhered to where Bank information assets are involved.
3.18 Aplicações de Negócio	3.18 Business Applications
a. Os controlos de segurança devem ser incorporados para proteger a confidencialidade e a integridade da informação quando esta é capturada ou carregada, processada e gerada por estas aplicações.	a. Security controls must be incorporated to protect the confidentiality and integrity of information when it is captured or loaded into, processed by and output from these applications.
b. Os controlos de segurança devem ser incorporados para proteger a disponibilidade de informação, fornecendo capacidade adequada para lidar com os volumes de trabalho normais e máximos através de processos de monitoramento e alerta.	b. Security controls must be incorporated to protect the availability of information by providing adequate capacity to cope with normal and peak volumes of work through processes for monitoring and alerting.
c. Os controlos de segurança devem proteger contra o acesso não autorizado, assegurando que os componentes principais "falhas com segurança" (ou seja, em caso de falha do sistema, a informação não é acessível a pessoas não autorizadas e não pode ser adulterada ou modificada).	c. Security controls must protect against unauthorised access by ensuring key components 'fail securely' (i.e. in the event of a system failure, information is not accessible to unauthorised individuals, and cannot be tampered with or modified).
d. O acesso a aplicações de negócios devem ser restritos apenas a pessoas autorizadas.	d. Access to business applications must be restricted to authorised persons only.
e. As aplicações de negócio críticos devem ser instaladas ou armazenadas (no caso de aplicações do tipo de mapa) num servidor central (por exemplo, para reduzir o risco de modificações acidentais e deliberadas e para ajudar a garantir que estes sejam copiados de forma centralizada).	e. Critical business applications must be installed or stored (in the case of spreadsheet type applications) on a central server (e.g. to reduce the risk of accidental and deliberate modification and to help to ensure that these are backed up centrally).
f. Deve haver acordos escritos antes da troca de informação ou software.	f. There must be written agreements in place before the exchange of information or software.
g. Terceiros devem seguir um processo aprovado para avaliar os riscos de informação e definir os controlos de risco e os requisitos de capacidade exigidos, com a contribuição do Banco.	g. Third Parties must follow an approved process to assess the information risks and define the required information risk controls and capacity requirements, with input from the Bank.

3.19 Aplicações Auto-Desenvolvidas do Usuário Final	3.19 End User Self Developed Applications
a. Somente o software aprovado ou licenciado pelo Banco deve ser usado para criar aplicações e armazenamento de dados auto-desenvolvidos para o usutilizador final.	a. Only approved or licensed software must be used to create end-user self-developed applications and data stores.
b. Todas as aplicações e armazenamento de dados auto-desenvolvidos do usuário final devem ser aprovadas pelo Banco antes de serem desenvolvidas.	b. All end-user self-developed applications and data stores must be approved before being developed.
c. Todas as aplicações e armazenamento de dados auto-desenvolvidos do usuário final devem ter um responsável identificado e documentado.	c. All end-user self-developed applications and data stores must have an identified and documented owner.
d. As alterações nas versões de produção de aplicações e armazenamento de dados auto-desenvolvidos do utilizador final devem ser submetidas a testes e gestão de lançamento de acordo com os princípios de gestão de alterações do Banco.	d. Changes to production versions of end-user self-developed applications and data stores must be subjected to testing and release management according to formal change management principles.
e. As aplicações e os armazenamentos de dados auto-desenvolvidos do utilizador final devem ser copiados e arquivados de acordo com os requisitos de resiliência, regulamentação e negócios combinados com o Banco.	e. End-user self-developed applications and data stores must be backed up and archived in accordance with the agreed Bank's business resilience, regulatory and business requirements.
f. Um registo de activos de informação deve indicar quando as aplicações ou armazenamento de dados auto-desenvolvidos do usuário final são desactivados. A informação deve ser removidas de forma segura antes de aplicações e armazenamentos de dados auto-desenvolvidos do usuário final serem de-comissionados.	f. An information asset register must indicate when the end-user self-developed applications or data stores have been decommissioned. Information must be securely removed before end-user self-developed applications and data stores are decommissioned.
3.20 Sistemas de Informação do Banco (por ex. e-mail, internet e intranet)	3.20 Bank Information Systems (e.g. e-mail, internet and intranet)
a. Colaboradores de Terceiros não devem usar os sistemas de informação do Banco de forma a prejudicar a produtividade do Terceiro e/ou a disponibilidade dos activos de informações do Banco.	a. Third-Party personnel must not use the Bank's information systems in a manner that adversely affects Third Party productivity and/or the availability of the Bank's information assets is prohibited.
b. Colaboradores de Terceiros devem usar os sistemas de comunicação do Banco de forma responsável e ética. Colaboradores de Terceiros não devem representar-se ou representar ao Banco de forma falsa ou enganosa ao usar essas ferramentas de negócios.	b. Third-Party personnel must use the Bank's communication systems in a responsible and ethical manner. Third Party personnel must not represent themselves or the Bank in a false or misleading way when using these business tools.
c. Exercer bom senso ao usar plataformas de redes sociais. O Terceiro deve agir de forma responsável e será responsabilizado por quaisquer acções não autorizadas nas redes sociais.	c. Exercise good judgment and common sense when using social media platforms. The Third Party must act responsibly and will be held accountable for any unsanctioned actions on social media sites.

d. Os colaboradores de Terceiros não devem divulgar qualquer informação confidencial ou de propriedade do Banco, clientes ou outros terceiros, sem autorização prévia.	d. Third-Party personnel must not disclose any of the Bank's, customers' or other third parties' confidential or proprietary information without prior authorisation.
3.21 Teletrabalho	3.21 Remote working
a. O Terceiro deve tomar medidas para proteger os activos de informaçõão do Banco manipulados em computação móvel e instalações de teletrabalho.	a. The Third Party must take steps to protect the Bank information assets handled on mobile computing and remote working facilities.
b. Qualquer trabalho remoto que envolvam os activos de informação do Banco deve ser aprovado pelo Banco.	b. Any remote working involving the Bank information assets must be approved by the Bank.
c. Qualquer dispositivo portátil (armazenamento ou computação) usado para teletrabalho deve ser seguro - de acordo com o que foi estabelecido com o Banco - e ter no mínimo, uma firewall pessoal e capacidade anti-malware adequada, se for um dispositivo informático.	c. Any Portable device (storage or computing) used for remote working must be secure – according to agreement with the Bank –and have a personal firewall and anti-malware capability enabled as a minimum if it is a computing device.
d. Todos os trabalhadores remotos devem ter cumprido os requisitos de triagem estabelecidos nesta política.	d. Any remote workers must have passed the screening requirements set out in this policy.
3.22 Computação Móvel	3.22 Mobile Computing
a. Os funcionários e subcontratados de Terceiros nunca devem deixar dispositivos móveis (por exemplo, laptop, palmtops e smartphones) sem supervisão, a menos que estejam devidamente protegidos fisicamente (por exemplo, bloqueio de cabo) e logicamente (por exemplo, activar a senha de activação e a tela de bloqueio).	a. Third Party employees and sub-contractors must never leave mobile devices (e.g. laptop, palmtops and smart phones) unattended, unless properly secured both physically (e.g. cable lock) and logically (e.g. enable power-on password and lock screen).
b. Sempre que possível, os dispositivos móveis devem ser protegidos com senhas, biometria, tokens, senhas de controlo de acesso, software de protecção contra malware, e/ou criptografia, conforme acordado com o Banco.	b. Where possible, mobile devices must be protected with power-on passwords, biometrics, tokens, access control passwords, malware protection software, containerisation and/or encryption as agreed with the Bank.
c. O acesso aos activos de informação do Banco por meio de dispositivos de propriedade pessoal deve ser aprovado pelo Banco e gerido através do uso de controlos do Banco, ou semelhante.	c. Access to Bank information assets via personally owned devices must be approved by the Bank and managed through the use of Bank controls, or similar.
d. Os dispositivos móveis devem ser fisicamente protegidos e resguardados quando em uso, armazenados e/ou transportados.	d. Mobile devices must be physically protected and secured when in use, stored and/or transported.
e. Somente os activos de informação com controlos aplicados e acordados pelo Banco devem ser usados para aceder a activos de informação do Banco.	e. Only information assets with Bank agreed controls applied must be used to access Bank information assets.

f. Deve haver cuidado quando se utilizam dispositivos móveis em locais públicos ou áreas desprotegidas fora das instalações do Banco, para evitar o risco de ser visto ou ouvido por pessoas não autorizadas.	f. Care must be taken when using mobile devices in public places or unprotected areas outside of the Bank's premises, to avoid the risk of information being seen or overheard by unauthorised people.
3.23 Terceirização (por exemplo, computação em nuvem, ambiente hospedado, armazenamento fora do local, etc.)	3.23 Outsourcing (e.g. cloud computing, hosted environment, off-site storage, etc.)
a. Todos os acordos de terceirização devem ser avaliados de acordo com os critérios de materialidade estabelecidos abaixo:	a. All outsourcing arrangements must be assessed against the materiality criteria set out below:
i. O impacto financeiro e operacional se a actividade de negócio ou a função for interrompida.	i. The financial and operational impact if the business activity or function is interrupted.
ii. A influência quantitativa ou qualitativa que terá sobre uma linha de negócio significativa do Banco.	ii. The quantitative or qualitative influence it will have on a significant line of business of the Bank.
iii. O impacto de reputação se o Terceiro não realizar dentro do tempo acordado.	iii. Reputational impact if the Third-Party does not perform within the time given.
iv. O custo do acordo de terceirização como uma percentagem das despesas totais.	iv. The cost of the outsourcing arrangement as a percentage of total expenses.
v. Quão difícil será e quanto tempo demorará a encontrar um Terceiro alternativo ao invés de ter o Banco a desempenhar a própria actividade.	v. How difficult it will be and how long it will take to find an alternative Third-Party as opposed to having the Bank do the activity itself.
vi. A capacidade de cumprir os requisitos regulamentares ou o impacto nos processos de supervisão do regulador.	vi. Ability to meet regulatory requirements or impact on the regulator's supervisory processes.
vii. O número de acordos de terceirização realizados com um único fornecedor de serviços que, em conjunto, pode ser visto como materiais para o Banco.	vii. The number of outsourcing agreements held with a single service provider which together may be seen as material to the Bank.
viii. Impacto nos objectivos estratégicos do Banco se o Terceiro falhar.	viii. Impact on the strategic objectives of the Bank if the Third-Party fails.
ix. Perdas potenciais para os clientes do Banco ou de outras pessoas se o Terceiro falhar.	ix. Potential losses to customers of the Bank or other persons if the Third-Party fails.
x. Afiliação ou outra relação entre o Banco e o Terceiro.	x. Affiliation or other relationship between the Bank and the Third-Party.
xi. A influência no mercado financeiro e concorrentes, bem como o potencial de risco sistémico para o mercado financeiro como um todo.	xi. The influence on the financial market and competitors as well as the potential for systemic risk to the financial market as a whole.
xii. A jurisdição legal em que o contracto de terceirização cairia.	xii. The legal jurisdiction in which the outsourcing agreement would fall.

b. A avaliação de diligência deve ser realizada em potenciais Terceiros antes de celebrar um contracto com eles, para avaliar o seu compromisso e a capacidade de cumprir pelo menos esta política ao longo do período de acordo.	b. Due diligence assessment must be conducted on prospective Third Parties before entering into a contract with them, to evaluate their commitment and ability to comply with at least this policy over the period of agreement.
c. O Terceiro deve permitir que exercícios de diligência (uma vez e/ou periódicos) sejam concluídos por uma área de negócio ou departamento autorizado do Banco para Terceiros que irão aceder os activos de informação do Banco, por ex., para verificar o cumprimento desta política de tempos em tempos, isto inclui os subcontratados de um Terceiro.	c. The Third-Party must permit due diligence exercises (once-off and/or periodic) to be completed by an authorised Bank business area or department for Third Parties who will access the Bank information assets e.g. to audit compliance with this policy from time to time, this includes the subcontractors of a Third-Party.
d. As avaliações de *due diligence* devem ser concluídas antes da transferência ou acesso aos activos de informação do Banco, ou ligação aos sistemas do Banco, pelo Terceiro ou seus colaboradores e subcontratados, por exemplo, apresentando prova de conformidade pelo Terceiro (por exemplo, certificações ou resultados de conformidade de melhores práticas da indústria).	d. Due diligence assessments must be completed prior to the transfer of or access to Bank information assets, or connection to the Bank's systems, by the Third Party or its employees and sub-contractors e.g. submitting proof of compliance by the Third Party (e.g. certifications or industry best practice compliance results).
e. Acções de recuperação para mitigar riscos identificados para Terceiros devem ser identificadas e implementadas a um nível aceitável (para o Banco), antes de qualquer compromisso contratual.	e. Remedial actions to mitigate identified risks for Third Parties, must be identified and implemented to an acceptable level (to the Bank), prior to any contractual engagements.
f. A garantia de que os activos de informação do Banco disponibilizados para o Terceiro serão tratados exclusivamente nos termos e condições especificados no contracto entre o Banco e o Terceiro.	f. The assurance that the Bank's information assets made available to the Third-Party will be handled solely within the terms and conditions specified in the agreement between the Bank and the Third-Party.
3.24 Consciencialização e Educação	3.24 Awareness and Education
a. O Terceiro deve fornecer informações adequadas sobre o risco de informação e consciencialização aos seus funcionários e subcontratados com acesso aos activos de informação do Banco.	a. The Third-Party must provide appropriate information risk awareness and education to its employees and sub-contractors with access to the Bank information assets.
b. O Terceiro deve consciencializar os seus colaboradores e subcontratados no que se refere a segurança da informação e aos controlos de risco exigidos por esta política, bem como aos contractos e acordos que o Terceiro possui com o Banco.	b. The Third-Party must educate its employees and sub-contractors with regards to the information security and risk controls required by this policy, and the contracts and agreements the Third-Party has with the Bank.
3.25 Monitoramento	3.25 Monitoring
a. Os processos devem estar em vigor para o monitoramento e registo de actividades realizadas durante o processamento dos activos de informação do Banco.	a. Processes must be in place for the monitoring and logging of activities undertaken during the processing of the Bank information assets.
b. As actividades monitorizadas devem, sempre que possível, ser atribuídas a usuários individuais e, no mínimo, incluir:	b. Activities monitored must, wherever possible, be attributable to individual users and must, as a minimum, include:

i. Registos de acessos.	i. Access logs.
ii. Registos de acesso de utilizadores privilegiados.	ii. Privileged user access logs.
iii. Registos de erros.	iii. Error logs.
iv. Registos de alterações.	iv. Change logs.
c. Os registos devem ser:	c. Logs must be:
i. Armazenados e protegidos contra acesso não autorizado e alterações.	i. Stored and protected against unauthorized access and change.
ii. Mantidos e monitorizados de forma segura.	ii. Securely maintained and monitored.
iii. Revistos regularmente e tomadas acções apropriadas dependendo dos resultados da revisão.	iii. Reviewed regularly and appropriate actions taken dependent upon the results of the review.
3.26 Compliance	3.26 Compliance
a. Os terceiros devem assegurar que são cumpridas todas as obrigações legais, regulamentares e contratuais aplicáveis, bem como quaisquer normas de boas práticas da indústria exigidas, conforme especificado ou acordado com o Banco. No mínimo, o seguinte deve ser considerado:	a. Third Parties must ensure that they are compliant with all applicable statutory, regulatory and contractual obligations as well as any required industry best practice standards as may be specified or agreed with the Bank. At a minimum, the following must be considered:
i. Risco de Informação.	i. Information Risk.
ii. Segurança de TI.	ii. IT Security.
iii. Cibercrime e Ciber-Segurança.	iii. Cyber Crime and Cyber Security.
iv. Gestão de Risco de Serviços Financeiros.	iv. Financial Services Risk Management.
v. Praticas contra o Suborno e Corrupção.	v. Bribery and Corrupt practices.
vi. Anti-branqueamento	vi. Anti-money laundering.
vii. Anti-terrorismo.	vii. Anti-terrorism.
viii. Privacidade.	viii. Privacy and Data Privacy.
ix. Segurança de transações.	ix. Transaction security.
b. Os terceiros devem cumprir os requisitos relevantes decorrentes de acções de execução por órgãos aplicáveis (regulamentares ou legais).	b. Third Parties must comply with relevant requirements that stem from enforcement action by applicable bodies (regulatory or legal).
c. Os reguladores do Banco têm o direito de acesso aos activos de informação relacionados com o Banco em posse do Terceiro como consequência da própria informação e operações do Banco e seus subcontratados. Quando um pedido regulatório é recebido, o Bando deve ser notificado e o acesso ao regulador deve ser providenciado apenas com a autorização do Banco.	c. The Bank's regulators have the right of access to Bank related information assets in possession of the Third-Party as a consequence of the Bank's own information and operations and its subcontractors. When a regulatory request is received, the Bank must be notified and access to the regulator may only be provided with the Bank's authorisation.

4. EXCEPÇÕES	4. EXCEPTION
O desvio dos requisitos mínimos desta política deve ser enviado ao Responsável da Política e aprovado pelo Comité de Gestão de Risco. Todas as excepções a esta política devem ser formalmente registadas, rastreadas e analisadas pelo Comité e comunicadas as partes interessadas relevantes. Quaisquer excepções devem ter um plano de acção claro e a data de vencimento para que a excepção seja encerrada.	Deviation from the minimum requirements of this policy must be submitted to the Policy Owner and approved by the Risk Management Committee (RMC). All exceptions to this policy must be formally recorded, tracked and reviewed by the RMC, communicated to relevant stakeholders. Any exceptions must have a clear action plan and due date for the exception to be closed.
5. FUNÇÕES E RESPONSABILIDADES	**5. ROLES AND RESPONSIBILITIES**
5.1 Os Superiores Hierárquicos da Unidade de Negócio ("UN / BU - *Business Unit*") e da Área de Suporte ("AS / EF - *Enabling Function*") devem garantir que o pessoal do Terceiro e subcontratados	5.1 Bank Business Unit (BU) and Corporate Function (CF) Line Managers must ensure that Third Party personnel and sub-contractors:
a. Estão conscientes das suas responsabilidades em relação aos requisitos desta Política;	a. Are made aware of their responsibilities with regards to the requirements of this Policy.
b. Reconhecem, compreendem e assinam a Política de Uso Aceitável especificada;	b. Acknowledge, understand and sign the relevant policy acknowledgement form.
c. Os superiores hierárquicos devem nomear uma parte responsável que actuará como assessora de informação de risco / segurança da informação focal em assuntos relacionados com a política;	c. Line Managers must appoint a responsible party who will act as the focal information risk / information security advisor on policy related matters.
d. Certificar-se de que todos os recursos não permanentes reconhecem e assinam a referida política especificado anualmente como parte dos programas regulares de indemnização da casa;	d. Ensure that all non-permanent resources annually acknowledge and sign the relevant policy acknowledgement form as part of regular formalized, in-house compliance programmers.
e. Certificar-se de que as responsabilidades de risco de informação são especificadas;	e. Ensure that information risk responsibilities are specified.
f. Certificar-se que as avaliações de risco de informação e as revisões de diligência são conduzidas	f. Ensure that information risk assessments and due diligence reviews are conducted.
g. Dar informações sobre incidentes de risco e quebras ao serviço de apoio de TI (EXT 2600), ao superior hierárquico e ao gestor de risco imediatamente.	g. Report information risk incidents and information breaches to the Bank IT Service Desk (EXT 2600), Line Manager and Embedded Risk Manager immediately.
h. Reassinar o formulário de reconhecimento da política relevante no encerramento de serviços para lembrar as suas responsabilidades de proteger os activos de informação do Banco. Consultar a tabela abaixo para os intervalos de interacção que exigem aprovações.	h. Re-sign the relevant policy acknowledgment form on termination of services to serve as a reminder of their responsibilities to protect the Bank's information assets. See table below for engagement intervals that require signoffs.

Período de Interação / Engagement period	**Requisitos de autorização / Signoff requirements**
1 dia / day – 6 meses / months	Assinado na entrada e término / Sign at engagement and termination

1 mês / month – 1 ano / year	Assinado na entrada, fim de ano e término / Sign at engagement, year end and termination
+ 1 ano / year	Assinado na entrada, fim de ano e término / Sign at engagement, year end and termination
i. Concordam com o Terceiro em medidas alternativas ou compensatórias para proteger os activos de informação do Banco quando o Terceiro não pode cumprir esta política (por exemplo, o Banco pode fornecer os recursos do Terceiro com equipamentos informáticos geridos pelo Banco).	i. Agree with the Third-Party on alternate or compensating measures to protect Bank information assets where the Third Party cannot comply with this policy (e.g. the Bank may provide Third Party resources with Bank managed computer equipment.
5.2 Gestor de Risco de Informação deve:	5.2 Information Risk Manager must:
a. Certificar-se de que esta política permanece apta para fins e práticas para implementação em todo o Banco.	a. Ensure that this policy remains fit for purpose and practical for implementation across the Bank.
b. Manter uma base de dados de excepções (desvios ou renúncias) às políticas de Risco de Informação.	b. Maintain a database of exceptions (deviations or waivers) to Information Risk policies.
c. Supervisionar a conformidade com esta política.	c. Oversee compliance with this policy.
c. SupervisonarFornecer controlo sobre a implementação desta política.	d. Provide oversight, ongoing assurance and reporting on the implementation of this policy.
e. Garantir que as formações e campanhas de sensibilização sobre risco de informação são conduzidas com as partes internas interessadas	e. Ensure that Information Risk related training and awareness is conducted with internal stakeholders.
5.3 A Direcção de Engenharia deve:	5.3 Engineering must:
a. Garantir que o acesso apenas é activado após a confirmação/verificação de contractos/SLAs assinados, reconhecimento por escrito desta política e recebimento de um pedido de acesso autorizado.	a. Ensure that access is only activated upon confirmation/verification of signed contracts / SLAs, signed acknowledgement of this policy and receipt of an authorised access request.
5.4 O Gestores de Risco Não-Financeiro devem:	5.4 Non-Financial Risk Managers must:
a. Facilitar a implementação desta política no Banco todo.	a. Facilitate the implementation of this policy across the Bank.
b. Facilitar a identificação de riscos de informação com as partes terceiras.	b. Facilitate the identification of Third-Party information risks.
c. Liderar a sensibilização desta política dentro das áreas de negócio.	c. Drive awareness on this policy within their Business Units.
5.5 Equipa de *Procurement* deve:	5.5 Procurement must:
a. Deve gerir o relacionamento com Terceiros para lidar com consultas e garantir uma comunicação adequada entre o Terceiro e o Banco.	a. Manage the relationship with Third Parties to handle enquiries and ensure appropriate communication between the Third-Party and the Bank

b. Incluir o reconhecimento desta política por Parte de Terceiras aos processos de Procurement e estruturas de trabalho.	b. Embed the acknowledgement of this policy, by Third Parties, into procurement processes and frameworks.
5.6 A Direcção de Pessoas e Cultura deve:	5.6 People and Culture must:
a. Incluir o reconhecimento desta política por parte de terceiros, aos processos e estruturas de trabalho	a. Embed the acknowledgement of this policy, by Third Parties, into People and Culture processes and frameworks.
5.7 Os funcionários de Terceiros devem:	5.7 Third Party personnel must:
a. Cumprir com os princípios e requisitos mínimos definidos nesta política.	a. Comply with the principles and minimum requirements defined in this policy.
b. Usar os activos de informação do Banco de forma apropriada e responsável.	b. Use the Bank's information assets appropriately and responsibly.
c. Reportar violações de segurança e ou o não cumprimento desta política.	c. Report security violations and / or non-compliance with this policy.
d. Devolver os activos de informação quando terminarem ou alterarem o contrato ou acordo de emprego. Cópias da informação do Banco devem ser apagadas / removidas de forma aceitável.	d. Return Bank information assets on termination or change of their employment contract or agreement. Copies of Bank information must be deleted / disposed of in an acceptable manner.
6. POLÍTICAS E PROCEDIMENTOS RELACIONADOS	**6. RELATED POLICIES AND PROCEDURES**
Os fornecedores devem fazer uso das práticas recomendadas da indústria, conforme apropriado para a sua indústria (por exemplo ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27036, e ISO/IEC 27015, NIST Privacy Framework and PCI DSS etc.).	Vendors should make use of industry best practices as appropriate to their industry (e.g. ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27036, ISO/IEC 27015 and 29100, NIST Privacy Framework and PCI DSS etc.).
7. CONSEQUÊNCIAS DA VIOLAÇÃO	**7. CONSEQUENCES OF VIOLATION**
Acção legal em conformidade com os contractos relevantes com o Terceiro pode ser executada contra Terceiros que não cumpram esta Política. Sempre que tal incumprimento constitua uma falta grave ou uma violação em termos dos contractos relevantes, pode resultar na rescisão do contracto ou acordo de serviço.	Legal action in line with the relevant contracts with the Third Party may be taken against Third Parties who do not comply with this Policy. Where such non-compliance constitutes gross misconduct or a breach in terms of the relevant contracts it may result in termination of the contract or service agreement.
8. DEFINIÇÕES	**8. DEFINITIONS**
Os seguintes termos definidos devem aplicar-se a esta Política:	The following defined terms shall apply to this Policy:
Medidas de segurança apropriadas: Isto significa que os controlos necessários devem ser aplicados para corresponder com a segurança, valor e classificação de privacidade dos activos de informações relevantes	Appropriate security measures: This means that the necessary controls must be applied in order to correspond with the security, value and privacy classification of the relevant information assets
Arquivo: Remover informações de uso operacional para serem armazenadas pelo Banco ou por um terceiro para fins de retenção.	Archive: Removing information from operational use to be stored by the Bank or by a third party for purposes of retention.

Back up: Copiar e arquivar informações para um segundo meio como precaução no caso de o primeiro meio falhar, para que ele possa ser usado para restaurar o original.	Back up: Copying and archiving of information to a second medium as a precaution in case the first medium fails, so that it may be used to restore the original.
Dados: A representação de factos, exto, números, gráfico, imagens, som ou vídeo.	Data: The representation of facts as text, numbers, graphics, images, sound or video. Added
Privacidade de Dados: Requisitos legais e melhores práticas relacionadas a privacidade e processamento de informação pessoal.	Data Privacy: Legal requirements and best practice relating to privacy and the processing of personal information. Added
Risco de Privacidade de Dados: Risco operacional, legal, tecnológico e outros associados ao processamento de informação pessoal.	Data Privacy Risk: Operational, legal, technology and other risks associated with the processing of personal information. Added
Violação de Privacidade de Dados: Ocorre quando existem motivos razoáveis para acreditar que o acesso aos dados foi adquirido por uma pessoa não autorizada ou conforme definido pela legislação aplicável sobre privacidade de dados.	Data Privacy Breach: Occurs where there are reasonable grounds to believe that access to PII was acquired by an unauthorized person or as defined by any other applicable data privacy legislation. Added
Titular dos Dados: uma pessoa ou entidade jurídica a quem as informações pessoais se relacionam ou que podem ser identificadas pelas PII (Informação Pessoalmente Identificável). Também conhecida como o conceito de PII.	Data Subject: A person or juristic entity to whom personal information relates, or who can be identified from PII. Also known as PII Principal. Added
Funcionários: Conforme informado pela Resolução relativa à Classificação Internacional Geral do Estatuto do Emprego (ICSE-93), o emprego no Banco Standard Bank deverá incluir o seguinte, independentemente das responsabilidades de trabalho, departamento e/ou localização específica e deve ser lido em conjunto com a Política Não Permanente e a Política de Relações de Emprego: • Funciários permanentes; • Funcionários não permanentes que contractam diretamente ao Standard Bank, denominados Contratados de Prazo Fixo (Standard Bank); • Recursos não permanentes incluem Contratos de Duração Fixa/Duração Limitada e Serviços Temporários. • O Banco reconhece que pode ser conjunta e gravemente responsável por qualquer recurso Não Permanente garantido através de um Terceiro como Empregador Secundário para os empregados não permanentes contratados através de um Terceiro, por exemplo. Serviço de Emprego Temporário (TES - *Temporary Employment Service*), que será considerado o principal Empregador desses empregados, em conformidade com a legislação específica do país. A definição de Emprego exclui Prestadores de Serviços Independentes (ISP - *Independent Services Providers*).	Employee: As informed by the Resolution concerning the General International Classification of the Status of Employment (ICSE-93), employment in Standard Bank shall include the following, regardless of specific job responsibilities, department and/or location and should be read in conjunction with the Non-Permanent Policy and Employment Relations Policy: • Permanent employees; • Non-permanent employees who contract directly to Standard Bank, termed Fixed Term Contractors (Standard Bank); • Non-permanent resources shall include Fixed Term Contract/Limited duration contracts and Temporary Services. • The Bank acknowledges that it may be jointly and severably liable for any Non-permanent resource secured via a Third Party as Secondary Employer for such non-permanent employees engaged through a Third Party I.e. Temporary Employment Service (TES) who shall be deemed to be the Primary Employer of such employees, in accordance with country specific legislation. For the purposes of this policy the definition of Employment shall include Independent Services Providers (ISP's).

Aplicações auto-desenvolvidas do usuário final: Qualquer aplicação (por exemplo, Mapas), armazenamento de dados (por exemplo, Microsoft Access) ou gerador de relatórios (por exemplo, Crystal Reports) que é desenvolvido por um usuário final e suporta processos comerciais.	End user self-developed applications: Any application (e.g. Spreadsheets), data store (e.g. Microsoft Access) or report generator (e.g. Crystal Reports) that is developed by an end-user and supports business processes.
Informação: A informação é uma colecção de dados em contexto. Sem contexto, os dados não têm sentido; criamos informações significativas interpretando o contexto em torno dos dados. Este contexto inclui: • O significado comercial de elementos de dados e termos relacionados • O formato no qual os dados são apresentados • O prazo representado pelos dados • A relevância dos dados para um determinado uso.	Information: Information is a collection of data in context. Without context, data is meaningless; we create meaningful information by interpreting the context around the data. This context includes: The business meaning of data elements and related terms • The format in which the data is presented The timeframe represented by the data The relevance of the data to a given usage.
Activos de informação: Um termo colectivo para informações e instalações associadas que inclui activos de software, activos físicos, serviços, pessoas (informações tácitas) e intangíveis (por exemplo, reputação e imagem da organização).	Information asset: A collective term for information and associated facilities that includes software assets, physical assets, services, people (tacit information) and intangibles (e.g. reputation and image of the organisation).
Evento de Informação: Um evento de risco relacionado aos activos de informação devido a uma excepção nas condições normais de trabalho.	Information event: An occurrence of risk relating to information assets due to an exception to normal operating conditions.
Incidente de informação: Qualquer evento que se materializa e tenha impacto na confidencialidade, integridade ou disponibilidade dos dados ou informação. Inclui incidentes de privacidade, o que significa que informação pessoal tenha sido comprometida ou indevidamente processada.	Information incident: Any event that materialises and impacts on the confidentiality, integrity or availability of information or data. It includes a privacy incident, meaning PII has been compromised or unlawfully processed.
Quebra do Apetite de Risco de Informação: Ocorre quando a confidencialidade, integridade ou disponibilidade de informação classificada como “Confidencial” e “Secreta” é comprometida.	Information Risk Appetite Breach: Occurs when the confidentiality, integrity or availability of “Confidential” and “Secret” classified information is compromised.

Recursos não permanentes: Qualquer recurso que não esteja envolvido num contrato permanente com o Standard Bank Bank. O Standard Bank Bank distingue entre 4 categorias diferentes, nomeadamente: Contrato a prazo fixo (Standard Bank); Contrato de prazo fixo (Serviço de Emprego Temporário); Serviços temporários (apenas África do Sul); e Provedores de Serviços Independentes, incluindo Contratados Independentes, Provedores de Serviços Profissionais e grandes empresas.	Non-permanent resources: Any resource who is not engaged in a permanent contract with the Standard Bank. The Standard Bank distinguishes between 4 different categories, namely: Fixed Term Contract (Standard Bank); Fixed Term Contract (Temporary Employment Service); Temporary Services (South Africa only); and Independent Service Providers including Independent Contractors, Professional Service Providers and large companies.
Informação de Identificação Pessoal: Qualquer informação que possa ser usada para identificar o principal/titular dos dados de Identificação Pessoal a quem essas informações se relacionam ou pode estar directa ou indirectamente ligada a um titular de dados de Identificação Pessoal. Inclui informações pessoais e informações pessoais especiais.	Personally Identifiable Information: Any information that can be used to identify the PII principal/data subject to whom such information relates or might be directly or indirectly linked to a PII principal/data subject. It includes Personal Information and Special Personal Information.
Informação pessoal: Informações relativas a uma pessoa identificável, física ou jurídica, incluindo, entre outras, informações relacionadas com a raça, género, sexo, estado civil, nacionalidade, origem étnica ou social, cor, orientação sexual, idade, saúde física ou mental, religião, crença, deficiência, idioma, nascimento, educação, número de identidade, número de telefone, e-mail, endereço postal ou de rua, informações biométricas e histórico financeiro, criminal ou de trabalho, bem como correspondência enviada pela pessoa que é implícita ou explícita de uma natureza privada ou confidencial ou correspondência adicional que revele o conteúdo da correspondência original.	Personal information: Information relating to an identifiable, natural or juristic person, including but not limited to, information relating to race, gender, sex, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, religion, belief, disability, language, birth, education, identity number, telephone number, email, postal or street address, biometric information and financial, criminal or employment history as well as correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence.
Princípio de menor privilégio: Filosofia de controle de acesso que dita que é permitido aos usuários o mínimo de direitos de acesso possível para desempenho das suas funções.	Principle of least privilege: An access control philosophy that states that users are granted the minimal access possible for the completion of their tasks.
Privacidade: Todos têm direito a privacidade, o que inclui o direito de protecção contra a colecção, retenção, disseminação e uso da informação pessoal ilegal.	Privacy: Everyone has the right to privacy which includes a right to protection against the unlawful collection, retention, dissemination and use of personal information. Added

Risco de Privacidade: A probabilidade de que o direito a privacidade dos titulares dos dados seja violado como resultado do processamento das suas informações pessoais.	Privacy Risk: The likelihood that data subjects' right to privacy will be infringed resulting from the processing of their personal information. Added
Processamento: Qualquer actividade que resulte numa mudança de conteúdo, localização, estado ou estágio de vida da informação.	Processing: Any activity that results in a change of content, location, state or life stage of information.
Informação secreta: Informações secretas são informações com mais restrições de acesso do que informações confidenciais, e a sua exposição a pessoas não autorizadas, também dentro da organização, pode causar danos significativos ao Banco. Exemplos de informações secretas são reuniões do conselho e outras informações da reunião executiva, planos estratégicos de negócios, senhas, informação privilegiada legalmente e informações sobre fusões e aquisições.	Secret information: Secret information is information with more restrictions on access than confidential information, and its exposure to unauthorised persons, also within the organisation, may cause significant harm to the Bank. Examples of Secret information are board meeting and other executive meeting information, business strategic plans, passwords, legally privileged information and merger and acquisition information.
Informação sensível: Esta é uma informação que, quando a sua confidencialidade, integridade ou disponibilidade é comprometida, haverá um impacto de risco inaceitável no Banco (ou seja, aspectos financeiros, operacionais, reputativos, estratégicos, legais ou regulatórios do risco). Este tipo de informação também pode ser informação que tenha sido definida como sensível em certas legislações. As informações sensíveis serão, pelo menos, classificadas como confidenciais e exigem uma melhor protecção do que a informação comum.	Sensitive information: This is information that when its confidentiality, integrity or availability is compromised there will be an unacceptable risk impact on the Bank (i.e. financial, operational, reputational, strategic, legal or regulatory aspects of risk). This type of information may also be information that has been defined as sensitive in certain legislation. Sensitive information will at least be classified as confidential and requires better protection than ordinary information.
Sensibilidade da informação: Esta é uma medida relativa do potencial impacto de risco inaceitável que o Banco pode sofrer se a confidencialidade, integridade ou disponibilidade de informações confidenciais forem comprometidas.	Sensitivity of information: This is a relative measure of the potential unacceptable risk impact the Bank may suffer if the confidentiality, integrity or availability of sensitive information is compromised.
Armazenar: O armazenamento é a retenção de informações por um período de tempo (às vezes chamado de informação em repouso), e pode variar de um pen drive USB, unidade de disco rígido local a uma rede de área de armazenamento.	Store: Storage is the retention of information for a period (sometimes termed information at rest), and can range from a USB stick, local hard disc drive to a storage area network.

Informação de Contacto / Contact Details:

Departmento / Departament: Risco Não-Financeiro/ Non-Financial Risk

Email: claudia.lima@standardbank.co.ao

Palavras-chave / Keywords:
Risco de informação / Information risk
Segurança de informação / Information security
Activos de informação / Information assets
Parte externa / External party
Parte terceira / Third party
Gestão de Risco de Terceiros / Third-Party Risk Management
Requisitos Contractuais / Contractual requirements
Privacidade de Dados / Data Privacy
Risco de Privacidade / Privacy Risk

9. Histórico de Revisões / Revision History

*Versão / Version no.	Propósito da revisão / Purpose of revision:	Data da revisão / Review date:	Data de efectividade / Effective date:	Sumário dos pontos-chave revistos / Summary of key revision points:
V1	Nova política / New policy	Abril / April 2018	1 Maio / May 2018	Princípios e afirmações de gestão de risco de informação aplicáveis à partes externas / Information risk management principles and statements applicable to external parties
V2	Revisão bí-annual / Bi-annual review	Abril / April 2018	Abril / April 2018	Responsabilidades, definições e garantia de alinhamento com a política de risco de informação do Banco / Responsibilities, definitions and ensured alignment with updated Bank information risk policy
V3	Revisão bí-annual / Bi-annual review	Abril / April 2020	Abril / April 2020	Mudança de responsável. Verificação do conteúdo de privacidade, actualização de responsabilidades e definições / Change in ownership. Verify privacy content, updated responsibilities and definitions
V4	Revisão bí-annual / Bi-annual review	Outubro / October 2022	Outubro / October 2022	Alterações na página de assinatura, responsabilidades e pequenas alterações de palavras para fins de esclarecimento. / Changes to signature page, responsibilities and minor word changes for clarification purposes.

10. POLICY ACKNOWLEDGEMENT

Instruções: por favor, complete e assine este formulário para reconhecer a aceitação desta política. Mantenha este formulário para mostrar ao Banco quando solicitado.
Este deve ser assinado por cada membro da Parte Terceira envolvido sob uma Solicitação de Serviço ou um Programa de Atribuição de Recursos, incluindo funcionários e subcontratados.

Confirmo que li e entendi esta Política e comprometo-me a aderir aos requisitos estipulados.

Nome: _____
ID Nº: _____
ID: _____(ID atribuído aos Recursos Não Permanentes)

Assinatura: _____
Data: _____

Departamento: _____
Representante SBA: _____

Assinatura do Representante SBA: _____
Data: _____