1. **PRIVACY AND DATA PROTECTION POLICY**

1.1 This privacy and data protection policy describes the personal information that CHASE gathers on or through the provision of the SOFTWARE and, where applicable our SERVICES, and how CHASE uses and processes such information.

1.2 This policy should help YOU understand how WE use YOUR personal information, it explains in detail the types of personal information CHASE collects, what CHASE uses it for and who CHASE may share it with. If YOU have any further questions about this policy or how CHASE handles YOUR personal information, which is not dealt with here, please contact US using the contact details below.

1.3 Where the legal basis of consent is used, this will be gathered freely, and CHASE will use clear, plain language that is easy to understand, and YOU will be able to remove YOUR consent at any point.

1.4 **Who is Chase**?

1.4.1 CHASE is the responsible party of all personal information and data that is collected and processed about YOU when YOU sign up to use OUR SOFTWARE and OUR SERVICES for the purposes of the Protection of Personal Information Act, 4 of 2013 ("**POPI**"). For the purposes of this EULA, "**PERSONAL INFORMATION**" means personal information as defined in POPI.

1.4.2 Where YOU use the SOFTWARE and process the PERSONAL INFORMATION of YOUR employees, customers, suppliers, contacts, contractors and/or prospects and/or the employees of YOUR customers, suppliers, contacts, contractors and/or prospects ("**SECONDARY INFORMATION**") using our SOFTWARE and/or store SECONDARY INFORMATION on YOUR own servers, YOU are considered to be the responsible party in respect of such PERSONAL INFORMATION and the provisions of clauses 1.14 and 1.16 will apply to YOU as the responsible party.

1.4.3 OUR company name is Chase Software (Pty) Ltd, registration number 2015/410552/07, incorporated in the Republic of South Africa ("**RSA**") and our registered offices are at 10 Morris Street West, Rivonia, 2128.

1.5 **What Personal Information does Chase Collect**

1.5.1 PERSONAL INFORMATION means information relating to YOU which allows CHASE to identify YOU.

1.5.2 If you choose to use the SOFTWARE and/or SERVICES, YOU must provide US with some PERSONAL INFORMATION so that CHASE can provide the SOFTWARE and/or deliver the SERVICES to YOU. The PERSONAL INFORMATION WE collect is limited to the level WE need to provide the SOFTWARE, deliver the SERVICES and is made up of the following categories:

1.5.2.1 names;

1.5.2.2 email addresses;

1.5.2.3 phone numbers;

1.5.2.4 company names;

1.5.2.5 company addresses;

1.5.2.6 tax information;

1.5.2.7 internet protocol (IP) addresses;

1.5.2.8 selected usernames and passwords used to access OUR SERVICES;

1.5.2.9 name and selected details of YOUR SYSTEM ADMINISTRATOR.

1.5.3 Other non-mandatory PERSONAL INFORMATION may also be gathered.

1.6 **Why do we Collect/Process Personal Information?**

1.6.1 CHASE collects/processes PERSONAL INFORMATION so that WE can provide the best possible experience when YOU. Any PERSONAL INFORMATION and data collected is used to administer and deliver OUR SOFTWARE and SERVICES.

1.6.2 In addition, CHASE will collect/process YOUR PERSONAL INFORMATION:

1.6.2.1 to comply with record retention requirements in accordance with various legislation in the RSA;

1.6.2.2 to respond to YOUR queries and complaints;

1.6.2.3 for testing and applying new product or system versions, patches, updates and upgrades, and resolving bugs and other issues that YOU have reported to US;

1.6.2.4 to send YOU communications required by law or which are necessary to inform YOU about OUR changes to the SOFTWARE and SERVICES. For example, updates to the EULA and/or this policy;

1.6.2.5 to comply with OUR contractual or legal obligations to share data with law enforcement;

1.6.2.6 for statistical and marketing analysis, systems testing, customer surveys, maintenance and development, or in order to deal with a dispute or claim. Note that WE may perform data profiling based on the PERSONAL INFORMATION that WE collect from YOU for statistical and marketing analysis purposes. Any profiling activity will be carried out with YOUR prior consent only and by making best endeavours to ensure that all PERSONAL INFORMATION it is based on is accurate. By providing any PERSONAL INFORMATION YOU explicitly agree that WE may use it to perform profiling activities in accordance with this policy;

1.6.2.7 to manage OUR relationship with YOU as OUR customer and to improve OUR services and enhance YOUR experience with US;

1.6.2.8 to protect YOUR vital interests or those of another person;

1.6.2.9 to protect OUR legitimate interests.

1.6.3 YOU are free to opt out at any time by emailing or writing to US using the contact details below. YOU acknowledge that by opting out, WE may not be able to provide YOU with the SOFTWARE and/or the SERVICES.

1.6.4 CHASE will only process YOUR PERSONAL INFORMATION where it has a legal basis to do so. The legal basis will depend on the reasons for which WE have collected and need to use YOUR PERSONAL INFORMATION.

1.7 **Rational for Processing**

CHASE will process PERSONAL INFORMATION on the basis that WE have obtained YOUR consent to do so in accordance with our contractual obligations to fulfil which require such processing, and because WE have a legitimate interest as the legal basis to do so.

1.8 **Retention of Personal information**

1.8.1 The retention and/or deletion of YOUR PERSONAL INFORMATION will be subject to:

1.8.1.1 OUR compliance with any legal obligations that WE may be subject to with regards to the retention and/or deletion of PERSONAL INFORMATION; and/or

1.8.1.2 any contractual obligations that WE are bound to.

1.8.2 Subject to clause 1.8.1:

1.8.2.1 CHASE will not retain your PERSONAL INFORMATION for longer than is necessary to fulfil the purpose it was collected/ processed for. To determine the appropriate retention period, CHASE considers the amount, nature and sensitivity of the PERSONAL INFORMATION, the purposes for which WE process it and whether WE can achieve those purposes through other means. WE must also consider periods for which WE might need to retain PERSONAL INFORMATION in order to meet OUR legal obligations or to deal with complaints, queries and to protect OUR legal rights in the event of a claim being made;

1.8.2.2 upon the termination of the CHASE AGREEMENT, WE will, at YOUR written election, either destroy or return YOUR PERSONAL INFORMATION to YOU. When CHASE no longer needs YOUR PERSONAL INFORMATION, CHASE will securely delete or destroy it. WE will also consider if and how WE can minimise over time the PERSONAL INFORMATION that WE use, and if WE can de-identity YOUR PERSONAL INFORMATION so that it can no longer be associated with YOU or identify YOU, in which case WE may use that information without further notice to YOU.

1.9 **Marketing**

CHASE would like to send YOU information about products and services of CHASE which may be of interest to YOU. YOU have a right at any time to stop US from contacting YOU for marketing purposes by sending US an email with YOUR request or by unsubscribing by opting out of OUR communications.

1.10 **Your rights**

1.10.1 **Accessing or Rectifying your Personal Information**

WE want to make ensure that YOUR PERSONAL INFORMATION is accurate and up to date and YOU have the right to request a copy and update the PERSONAL INFORMATION that WE hold about YOU. YOU may ask us to correct or remove information YOU think is inaccurate by emailing or writing to US using the contact details in clause 1.18.

1.10.2 **Deletion**

Subject to clause 1.8.1, YOU may ask CHASE to delete or remove PERSONAL INFORMATION where there is no good reason for CHASE continuing to process it. YOU also have the right to ask US to delete or

remove YOUR PERSONAL INFORMATION where YOU have exercised YOUR right to object to processing (see below).

1.10.3 **Object to Processing**

YOU may object to OUR processing of YOUR PERSONAL INFORMATION where WE are relying on a legitimate interest (or that of a third-party) and there is something about YOUR particular situation which makes YOU want to object to processing on this ground. YOU also have the right to object where WE are processing YOUR PERSONAL INFORMATION for direct marketing purposes by unsubscribing by opting out of OUR marketing communications.

1.10.4 **Object to Automated Decision-Making Including Profiling**

YOU can object to being the subject of any automated decision-making or US using YOUR PERSONAL INFORMATION or profiling of YOU.

1.10.5 **Restriction of processing**

YOU may ask US to suspend the processing of PERSONAL INFORMATION about YOU, for example if YOU want US to establish its accuracy or the reason for processing it.

1.10.6 **Withdrawal of Consent**

1.10.6.1 Where YOU have provided YOUR consent to the collection, processing and/or transfer of YOUR PERSONAL INFORMATION for a specific purpose, YOU have the right to withdraw your consent for that specific processing at any time by emailing or writing to US using the contact details in clause 1.18.

1.10.6.2 Once WE have received notification that YOU have withdrawn your consent, WE will no longer process YOUR PERSONAL INFORMATION for the purpose or purposes YOU originally agreed to, unless CHASE has another legitimate basis for doing so in law.

1.10.6.3 YOU acknowledge that by withdrawing YOUR consent:

1.10.6.3.1 WE may discontinue providing the SOFTWARE and the SERVICES to YOU if WE required YOUR PERSONAL INFORMATION to deliver OUR SOFTWARE and SERVICES; and

1.10.6.3.2 YOU authorise US to uninstall the SOFTWARE from YOUR device and revoke YOUR access to OUR HOSTED SERVER.

1.10.7 **Portability**

YOU may wish to port YOUR PERSONAL INFORMATION to another platform. This enables YOU to take your PERSONAL INFORMATION from US in an electronically useable format and to be able to transfer YOUR PERSONAL INFORMATION to another party in an electronically useable format.

1.10.8 If YOU want to exercise any of YOUR rights, please email or write to us at the addresses in clause 1.18.

1.10.9 YOU will not have to pay a fee to access YOUR PERSONAL INFORMATION (or to exercise any of the other rights). However, CHASE may charge a

reasonable fee if YOUR request for access is clearly unfounded or excessive. Alternatively, WE may refuse to comply with the request in such circumstances.

1.11 **To Whom We Disclose Personal information**

Except as described in this policy, CHASE will not intentionally disclose YOUR PERSONAL INFORMATION that CHASE collects or stores via OUR SERVICES to any third-parties without YOUR consent. WE may disclose PERSONAL INFORMATION to third-parties if YOU consent to us doing so, as well as in the following circumstances:

1.11.1 **Unrestricted Information**

Any information that YOU voluntarily choose to include in a public area of OUR SERVICES, such as a public profile page, will be available to any visitor or user of OUR services who accesses that content.

1.11.2 **Group Companies**

Subject to the security restrictions on overseas transfers as set out in clause 1.11.4, YOUR PERSONAL INFORMATION may be shared with other companies within the CHASE group, both locally and internationally ("**GROUP COMPANIES**").

1.11.3 **Service providers**

1.11.3.1 CHASE works with third-party service providers ("**SERVICE PROVIDERS**") who provide, for example, email hosting, core corporate applications, web hosting, maintenance, and other services to CHASE in order for US to provide the SOFTWARE and deliver the SERVICES to YOU. These SERVICE PROVIDERS may have access to, or process YOUR PERSONAL INFORMATION as part of providing these services to CHASE. WE limit the information provided to these SERVICE PROVIDERS to that which is reasonably necessary for them to perform their functions, and OUR contracts with them require them to maintain the confidentiality of such information.

1.11.3.2 OUR service providers include Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin, 18, D18 P521, Ireland, provider of hosting and storing applications and associated data.

1.11.3.3 If WE ever move the location of OUR servers, WE will notify YOU thereof in writing.

1.11.4 **Overseas transfers**

1.11.4.1 The PERSONAL INFORMATION that YOU provide may be transferred to countries outside of the RSA, that do not have similar protections in place regarding YOUR PERSONAL INFORMATION and restrictions on its use as set out in this policy. However, CHASE will take steps to ensure adequate protections are in place to ensure the security of YOUR PERSONAL INFORMATION. By submitting YOUR PERSONAL INFORMATION, YOU consent to these transfers for the purposes specified above.

1.11.4.2 WE may transfer YOUR PERSONAL INFORMATION to the following which are located outside the RSA as follows:

1.11.4.2.1 Chase Software Limited, 2015/410552/07, for the purposes of providing the SOFTWARE and/or the SERVICES;

1.11.4.2.2 Chase Software PTE Limited (Singapore) (group company);

1.11.4.2.3 Afrihost SP (Pty) Ltd, 376 Rivonia Boulevard, Sandton, Gauteng, South Africa, Provider of and Web Hosting; SurveyMonkey, One Curiosity Way, San Mateo, CA 94403, USA, provider of survey tool to gain feedback from key stakeholders on satisfaction of service;

1.11.4.2.4 Atlassian, Level 29, 363 George Street, Sydney, NSW, 2000, Australia, provider of tool for knowledge base, issue tracking and project management;

1.11.4.2.5 Godaddy.com, 14455 N Hayden Rd Ste 226., Scottsdale, AZ 85260-6993, USA, provider of SSL (Secure Sockets Layer) certificates;

1.11.4.2.6 Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin, 18, D18 P521, Ireland.

1.11.4.3 CHASE is bound by the data protection laws of the RSA. You can obtain a copy of POPI at http://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf.

1.11.4.4 If CHASE transfers YOUR PERSONAL INFORMATION to any other countries, WE will put procedures and/or contractual obligations in place to ensure that YOUR PERSONAL INFORMATION receives at least a similar level of protection as set out by POPI.

1.11.5 **Non-Personally Identifiable Information**

WE may make non-personally-identifiable information available to third-parties for various purposes. This data maybe automatically-collected and would be analysed to create an aggregated view of the data and ensure the reported information was anonymous.

1.11.6 **Law Enforcement, Legal Process and Compliance**

CHASE may disclose PERSONAL INFORMATION or other information if required to do so by law or in the good-faith belief that such action is necessary to comply with applicable laws, in response to a court order, judicial or other government subpoena or warrant, or to otherwise co-operate with law enforcement or other governmental agencies, or if such disclosure is necessary to protect YOUR rights and/or the rights of others.

1.11.7 **Change of Ownership**

CHASE may disclose or otherwise transfer YOUR PERSONAL INFORMATION to an acquirer, successor or assignee as part of any merger, acquisition, debt financing, sale of assets, or similar transaction, as well as in the event of an insolvency, liquidation, business rescue proceeding, administrative process, in which information is transferred to one or more third-parties as one of OUR business assets and only if the recipient of the PERSONAL INFORMATION commits to a privacy policy that complies with POPI.

1.12 **Our Data Security**

1.12.1 WE have implemented appropriate technical, physical and organisational measures to protect PERSONAL INFORMATION against accidental or unlawful destruction or accidental loss, damage, alteration, unauthorised disclosure or access as well as all other forms of unlawful processing (including, but not limited to, unnecessary collection) or further processing.

1.12.2 WE use the following security procedures, technical and organisational measures to safeguard YOUR PERSONAL INFORMATION:

1.12.2.1 OUR primary use and storage of PERSONAL INFORMATION is on OUR own SOFTWARE which is highly encrypted and secure. All transfers of information are encrypted between OUR HOSTED SERVER and YOUR device. Where YOU use YOUR own servers to store PERSONAL INFORMATION, YOU will be the responsible party.

1.12.2.2 In cases where PERSONAL INFORMATION is being processed in other countries (except as set out above) or by third-parties, a data protection assessment will be performed to ensure that YOUR data is always secured.

1.12.2.3 OUR application platform is hosted in ISO 27001 certified secure data centres in the Northern Europe Region (Dublin, Ireland). If WE ever move the location of OUR servers, WE will notify YOU thereof in writing.

1.12.2.4 Firewalls, intrusion detection and prevention, anti-virus and anti-malware and backup and disaster recovery is in place to prevent data loss or deletion.

1.12.2.5 OUR offices and data centres are secured with an alarm system, access control and closed-circuit television.

1.12.2.6 OUR applications are engineered by following industry standards to minimise security vulnerabilities and are updated on a regular basis.

1.12.2.7 Intrusion detection and prevention secures the network traffic to the servers and applications.

1.12.2.8 Anti-malware and anti-virus software is deployed to all of OUR servers and regularly scan and update with the anti-malware and virus signatures.

1.12.2.9 WE regularly apply critical, security patches and firmware updates to operating systems and physical hardware to minimise the risk of vulnerabilities.

1.12.2.10 OUR employees undergo background screening and selection processes, with a restricted list of employees having access to secure areas of the applications, databases and physical infrastructure. The access by OUR employees and/or agents to the SOFTWARE, SERVICES and secure areas is logged and auditable.

1.12.2.11 WE will use all reasonable efforts to safeguard YOUR PERSONAL INFORMATION. However, YOU should be aware that the use of the internet is not entirely secure and for this reason CHASE cannot guarantee the security or integrity of any PERSONAL INFORMATION which is transferred from YOU or to YOU via the internet.

1.12.2.12 WE limit access to YOUR PERSONAL INFORMATION to those who have a genuine business need to know it. Those processing

YOUR PERSONAL INFORMATION will do so only in an authorised manner and are subject to a duty of confidentiality.

1.12.2.13 WE have procedures in place to deal with any suspected data security breach. WE will notify you and any applicable regulator of a suspected data security breach where WE are legally required to do so.

1.12.2.14 WE use Microsoft products including Microsoft Dynamics NAV which have data encryption and the privacy notice can be seen using the following link https://privacy.microsoft.com/en-gb/privacystatement. If the CLIENT has requested a Microsoft NAV product, YOU are deemed to be bound to the Microsoft privacy statement.

1.13 **Security Compromises**

1.13.1 WE promptly evaluate and respond to incidents that create suspicion of or indicate unauthorized access to or handling of YOUR PERSONAL INFORMATION.

1.13.2 If WE become aware of and determine that an incident ("**SECURITY COMPROMISE**") involving YOUR PERSONAL INFORMATION qualifies as a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, YOUR PERSONAL INFORMATION transmitted, stored or otherwise processed on OUR systems that compromises the security, confidentiality or integrity of such PERSONAL INFORMATION, WE will report such breach to YOU and the Regulator as soon as reasonably possible after the discovery of the SECURITY COMPROMISE.

1.13.3 OUR notification to YOU of the SECURITY COMPROMISE will be in writing and communicated in at least one of the following ways:

1.13.3.1 posted to YOUR last know physical or postal address;

1.13.3.2 emailed to YOUR last known email address;

1.13.3.3 prominently published on OUR website;

1.13.3.4 published in the news media; or

1.13.3.5 as may be directed by the Regulator.

1.13.4 Our notification to YOU of the SECURITY COMPROMISE will, at a minimum, include the following:

1.13.4.1 a description of the possible consequences of the SECURITY COMPROMISE;

1.13.4.2 a description of the measures that WE will take to address the SECURITY COMPROMISE;

1.13.4.3 a recommendation with regard to the measures that YOU should take to mitigate the possible adverse effects of the SECURITY COMPROMISE; and

1.13.4.4 if known, the identity of the unauthorised person who may have accessed or acquired YOUR PERSONAL INFORMATION.

1.14 **Secondary Information**

1.14.1 **Processing Your Secondary Information**

1.14.1.1 If YOU are using OUR hosted server to store SECONDARY INFORMATION, then YOU are the responsible party and we are the processor under POPI. Access to YOUR SECONDARY DATA is restricted by the users YOU allow access to as well as OUR support and engineering staff that need access in order to provide the SERVICES to YOU.

1.14.1.2 The categories and types of SECONDARY INFORMATION that WE may process on YOUR behalf are:

1.14.1.2.1 the names, addresses and contact details of YOUR employees, customers, suppliers, contacts, contractors and/or prospects;

1.14.1.2.2 the accounting system debtor information of YOUR customers, suppliers, contacts, contractors and/or prospects (this includes the debtor's name, address, contact details, registration number and address VAT number); and

1.14.1.2.3 the names, titles, designations, contact details and birthdays of the employees/representatives of YOUR customers, suppliers, contacts, contractors and/or prospects with whom YOU have contact.

1.14.1.3 WE will only perform processing activities that are necessary and relevant to render OUR SERVICES to YOU. WE will update this policy from time to time if there are any changes to the categories and types of SECONDARY INFORMATION that WE may process on YOUR behalf.

1.14.1.4 WE will maintain the documentation of all of OUR processing activities.

1.14.2 **Instruction**

1.14.2.1 WE will only act and process SECONDARY INFORMATION in accordance with YOUR written instructions ("**INSTRUCTIONS**"). YOUR INSTRUCTIONS at the time when YOU conclude YOUR CHASE AGREEMENT with US will be that WE may process SECONDARY INFORMATION with the purpose of:

1.14.2.1.1 rendering OUR SERVICES to YOU in accordance with the terms of the CHASE AGREEMENT; and

1.14.2.1.2 for statistical and marketing analysis, systems testing, customer surveys, maintenance and development, or in order to deal with a dispute or claim;

1.14.2.1.3 performing data profiling based on the SECONDARY INFORMATION for statistical and marketing analysis purposes. Any profiling activity will be carried out with YOUR prior consent only and by making best endeavours to ensure that all SECONDARY INFORMATION it is based on is accurate. By providing any SECONDARY INFORMATION YOU explicitly agree that WE may use it to perform profiling activities in accordance with this policy

1.14.2.2 It is YOUR obligation to ensure that any SECONDARY INFORMATION that YOU transfer to US is processed by YOU in accordance with applicable legislation (including POPI), including the legislative requirements regarding the lawfulness of processing.

1.14.2.3 If at any time WE consider YOUR INSTRUCTIONS to be in conflict with applicable data protection legislation, WE will notify YOU thereof without undue delay.

1.14.3 **Confidentiality**

1.14.3.1 WE will treat all the SECONDARY INFORMATION as strictly confidential information. SECONDARY INFORMATION may not be copied, transferred or otherwise processed in conflict with YOUR INSTRUCTIONS unless YOU have agreed thereto in writing.

1.14.3.2 OUR employees and the employees of OUR GROUP COMPANIES (collectively, "**GROUP EMPLOYEES**") as well as OUR SERVICE PROVIDERS who have access to and process YOUR SECONDARY INFORMATION will be subject to an obligation of confidentiality that ensures that they treat all SECONDARY INFORMATION with strict confidentiality

1.14.4 **Security and Sharing of Secondary Information**

1.14.4.1 The security measures set out in clause 1.12 of this policy will apply to SECONDARY INFORMATION.

1.14.4.2 SECONDARY INFORMATION may be shared throughout the CHASE GROUP (both locally and internationally subject to the security restrictions on overseas transfers as set out in clause 1.11.4). Any such transfer will be done on the basis that access to SECONDARY INFORMATION is restricted to only GROUP EMPLOYEES to whom it is necessary and relevant to process the SECONDARY INFORMATION in order for US to render OUR SERVICES to YOU.

1.14.4.3 Any GROUP EMPLOYEES whose work includes processing the SECONDARY INFORMATION will only do so in accordance with YOUR INSTRUCTIONS.

1.14.4.4 Your SECONDARY INFORMATION may be exported from OUR system by OUR engineers if necessary for testing and OUR policies are in place to ensure that this data is immediately removed after any tests are completed.

1.14.4.5 WE work with SERVICE PROVIDERS who provide, for example, email hosting, core corporate applications, web hosting, maintenance, and other services to US in order for US to render OUR SERVICES to YOU. These SERVICE PROVIDERS may have access to, or process YOUR SECONDARY INFORMATION as part of providing those services to US. WE limit the information provided to these SERVICE PROVIDERS to that which is reasonably necessary for them to perform their functions, and OUR contracts with them require them to maintain the confidentiality of such information.

1.14.4.6 OUR SERVICE PROVIDERS include Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin, 18, D18 P521, Ireland, Provider of hosting and storing applications and associated SECONDARY INFORMATION.

1.14.4.7 All transfers of YOUR business data is encrypted between OUR servers and the devices YOU use to access OUR SOFTWARE. WE cannot be held responsible for the security of YOUR devices.

1.14.4.8 WE may disclose SECONDARY INFORMATION or other information if required to do so by law or in the good-faith belief that such action is necessary to comply with applicable laws, in response to a facially valid court order, judicial or other government subpoena or warrant, or to otherwise cooperate with law enforcement or other governmental agencies, or if such disclosure is necessary to protect YOUR rights and/or the rights of others.

1.14.5 **Rights of the Data Subjects**

1.14.5.1 If YOU receive a request from a data subject for the exercise of the data subject's rights POPI and/or any other applicable data protection legislation and the correct and legitimate reply to such a request necessitates OUR assistance, WE will assist YOU by providing the necessary information and documentation. WE will require reasonable time to assist YOU with such requests.

1.14.5.2 If WE receive a request from a data subject for the exercise of the data subject's rights under POPI and/or any other applicable data protection legislation and such request is related to the SECONDARY INFORMATION, WE will immediately forward the request to YOU. WE will not respond to any such request directly to the data subject.

1.14.6 **Secondary Information Breaches**

1.14.6.1 If a breach of the data security occurs that can lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to, SECONDARY INFORMATION transmitted, stored or otherwise processed on YOUR behalf ("**SECONDARY INFORMATION BREACH**"), WE will notify YOU thereof without undue delay of becoming aware thereof.

1.14.6.2 When we notify you of the SECONDARY INFORMATION BREACH, our notification will, at a minimum, include the following:

1.14.6.2.1 a description of the possible consequences of the SECONDARY INFORMATION BREACH;

1.14.6.2.2 a description of the measures that WE will take to address the SECONDARY INFORMATION BREACH

1.14.6.2.3 a recommendation with regard to the measures that you should take to mitigate the possible adverse effects of the SECONDARY INFORMATION BREACH; and

1.14.6.2.4 if known, the identity of the unauthorised person who may have accessed or acquired the SECONDARY INFORMATION.

1.14.6.3 In turn, YOU, as the controller, will be required to notify YOUR THIRD-PARTIES of any such SECONDARY INFORMATION BREACHES with regards to the applicable SECONDARY INFORMATION.

1.14.7 **Return or Deletion of Secondary Information**

1.14.7.1 The retention and/or deletion of YOUR SECONDARY INFORMATION will be subject to OUR compliance with any legal obligations that WE may be subject to with regards to the retention and/or deletion of SECONDARY INFORMATION and/or records as well as any contractual obligations that WE are bound to.

1.14.7.2 Subject to clause 1.14.7.1, upon the termination of the CHASE AGREEMENT, WE will, at YOUR written election, either destroy or return all SECONDARY INFORMATION to YOU. In addition, when WE no longer need the SECONDARY INFORMATION to provide OUR SERVICES, WE will securely delete or destroy it.

1.15 **Operators**

If WE engage third-party processors ("**OPERATORS**") to have access to YOUR PERSONAL INFORMATION and/or YOUR SECONDARY INFORMATION in order to assist in the provision OUR SERVICES, such OPERATORS will be subject to the same level of data protection and security and confidentiality as us under the terms of OUR agreement with YOU. WE will be responsible for our OPERATORS' compliance with the terms of this EULA and the CHASE AGREEMENT in so far as they are applicable.

1.16 **Personal Information and Secondary Information in Your Hosted Environment**

1.16.1 If YOU are using YOUR own or a third-party hosted environment to store and/or process information, then you are the responsible party under POPI and WE will not have access to YOUR PERSONAL INFORMATION and/or SECONDARY INFORMATION unless you specifically grant us such access. WE will require access to YOUR hosted environment to implement upgrades, new systems, customisations and/or fixes.

1.16.2 WE will not process and/or remove to YOUR PERSONAL INFORMATION and/or SECONDARY INFORMATION from your hosted environment without YOUR permission.

1.16.3 If WE remove to YOUR PERSONAL INFORMATION and/or SECONDARY INFORMATION from your hosted environment, it will be for the purposes of implementing new systems, upgrades and/projects with regards to our SERVICES. Once the implementation is complete WE will migrate all of YOUR PERSONAL INFORMATION and/or SECONDARY INFORMATION back onto YOUR hosted environment and we will delete all records and copies of YOUR PERSONAL INFORMATION and/or SECONDARY INFORMATION that was used for the implementation from our systems.

1.16.4 If requested by YOU, we will create a backup of YOUR PERSONAL INFORMATION and/or SECONDARY INFORMATION, which backup will be stored on YOUR hosted environment.

1.17 **Systems Operations Data Processing Terms**

"**SYSTEMS OPERATIONS DATA**" includes log files, event files, and other trace and diagnostic files, as well as statistical and aggregated information that relates to the use and operation of OUR SERVICES, and the systems and networks that the SERVICES run on.

1.17.1 **Responsibility and Purposes for Processing Personal Information and/or Secondary Information in Systems Operations Data**

1.17.1.1 CHASE is responsible for processing PERSONAL INFORMATION and/or SECONDARY INFORMATION that may be incidentally contained in SYSTEMS OPERATIONS DATA.

WE may collect or generate SYSTEMS OPERATIONS DATA for the following purposes:

1.17.1.1.1 to help keep OUR SERVICES secure, including for security monitoring and identity management;

1.17.1.1.2 to investigate and prevent potential fraud or illegal activities involving OUR systems and networks, including to prevent cyber-attacks and to detect bots;

1.17.1.1.3 to administer OUR back-up disaster recovery plans and policies;

1.17.1.1.4 to confirm compliance with licensing and other terms of use (license compliance monitoring);

1.17.1.1.5 research and development purposes, including to analyse, develop, improve and optimize OUR services;

1.17.1.1.6 to comply with applicable laws and regulations and to operate OUR business, including to comply with legally mandated reporting, disclosure or other legal process requests, for mergers and acquisitions, finance and accounting, archiving and insurance purposes, legal and business consulting and in the context of dispute resolution.

1.17.1.2 For PERSONAL INFORMATION and/or SECONDARY INFORMATION contained in SYSTEMS OPERATIONS DATA collected in the RSA, OUR legal basis for processing such information is OUR legitimate interest in performing, maintaining and securing OUR products and SERVICES and operating OUR business in an efficient and appropriate manner. PERSONAL INFORMATION and/or SECONDARY INFORMATION may also be processed based on OUR legal obligations or legitimate interest to comply with such legal obligations.

1.17.2 **Sharing personal information and/or Secondary Information Contained in Systems Operations Data**

1.17.2.1 PERSONAL INFORMATION contained in SYSTEMS OPERATIONS DATA may be shared as contemplated in clause 1.11.

1.17.2.2 SECONDARY INFORMATION contained in SYSTEMS OPERATIONS DATA may be shared as contemplated in clause 1.14.4.

1.17.2.3 When third-parties are given access to PERSONAL INFORMATION and/or SECONDARY INFORMATION contained in SYSTEMS OPERATIONS DATA, WE will take the appropriate contractual, technical and organisational measures to ensure, for example, that such data is only processed to the extent that such processing is necessary, consistent with this policy and in accordance with applicable law.

1.17.3 **Security**

CHASE has implemented appropriate technical, physical and organisational measures to protect PERSONAL INFORMATION and SECONDARY INFORMATION contained in the SYSTEMS OPERATIONS DATA against accidental or unlawful destruction or accidental loss, damage, alteration, unauthorised disclosure or access as well as all other forms of unlawful processing (including, but not limited to, unnecessary collection) or further processing.

1.17.4 **Rights of Data Subjects**

1.17.4.1 To the extent provided under applicable laws, YOU may request to access, correct, update or delete PERSONAL INFORMATION contained in SYSTEMS OPERATIONS DATA in certain cases, or otherwise exercise t YOUR rights as contemplated in clause 1.10 by sending US a request to do so at the address in clause 1.18.

1.17.4.2 If YOU receive a request from a data subject for the exercise of the data subject's rights under POPI and/or any other applicable data protection legislation with regards to SECONDARY INFORMATION contained in SYSTEMS OPERATIONS DATA and the correct and legitimate reply to such a request necessitates OUR assistance, WE will assist YOU by providing the necessary information and documentation. WE will require reasonable time to assist YOU with such requests.

1.17.4.3 If WE receive a request from a data subject for the exercise of the data subject's rights under POPI and/or any other applicable data protection legislation with regards to SECONDARY INFORMATION contained in SYSTEMS OPERATIONS DATA, WE will immediately forward the request to YOU. WE will not respond to any such request directly to the data subject.

1.18 **Contact us**

1.18.1 OUR company address is 10 Morris Street West, Rivonia, 2191

1.18.2 OUR postal address is PO Box 2200, Pinegowrie, 2123

1.18.3 OUR telephone number is 086 11 242 73

1.18.4 OUR email address is privacy@chasesoftware.co.za

1.19 **Contacting the Regulator**

1.19.1 If YOU have any complaints regarding OUR compliance with this policy, please contact us first. WE will investigate and attempt to resolve any complaints and disputes regarding OUR privacy practices.

1.19.2 If YOU feel that YOUR PERSONAL INFORMATION has not been handled correctly, or YOU are unhappy with OUR response to any requests you have made to us regarding the use of YOUR PERSONAL INFORMATION, YOU have the right to lodge a complaint with the Regulator.

1.19.3 You can contact them by going online to www.justice.gov.za (please note WE can't be responsible for the content of external websites). The Regulator's details are as follows:

Address: SALU Building, 316 Thabo Sehume Street, Pretoria, Ms Mmanoroke Mphelo, Telephone 012-406-4818

email: inforreg@justice.gov.za

1.20 **Changes To this Privacy and Data Protection Policy**

1.20.1 WE may change this policy from time to time and any changes will be communicated to YOU by way of an e-mail, a notice on OUR website and/or on OUR mobile app.

1.20.2 YOU will be requested to accept any changes to this policy if YOU wish to continue using the SERVICES. If YOU do not accept such changes YOU will not be able to access OUR SERVICES, system and/or SOFTWARE. If YOU do not want to agree to changes to this policy, YOU can request an account deletion. Note that YOUR refusal to accept any changes to this policy will not absolve YOU of YOUR obligations in terms of the CHASE AGREEMENT.

1.20.3 This privacy policy was last updated on 2018/07/02.

1.21 **Limitation of Liability for Privacy and Data Protection**

1.21.1 **Whilst CHASE uses adequate security and technological measures to safeguard YOUR PERSONAL INFORMATION, CHASE will not be liable for any breach or compromise of PERSONAL INFORMATION and/or breach of privacy beyond the reasonable control of CHASE and which may include, but is not limited to:**

1.21.1.1 **acts of terrorism, cyber-terrorism, cyber-extortion, cyber-attacks, viruses, malware, malicious code, logic bombs, spyware, worms, trojan horses, hacking, vis-majors, criminal actions by third-parties unrelated to CHASE;**

1.21.1.2 **network disruptions beyond CHASE'S reasonable control and which may occur on YOUR computer systems and any failure by YOU or YOUR service providers to ensure that you implement adequate security safeguards to protect YOUR PERSONAL INFORMATION and SECONDARY INFORMATION on YOUR computer systems and devices;**

1.21.1.3 **unauthorised user access by YOU and password protection breaches which is no fault on the part of CHASE;**

1.21.1.4 **where YOU are the responsible party and host YOUR own PERSONAL INFORMATION on YOUR own servers or use YOUR own service providers to host YOUR PERSONAL INFORMATION and/or SECONDARY INFORMATION and any breach is not caused by any fault of CHASE.**

1.22 **Your Obligations in terms of this Privacy and Data Protection Policy**

1.22.1 **YOU warrant in favour of CHASE that YOU have obtained the consent of any third-party for the use of that third party's PERSONAL INFORMATION and/or SECONDARY INFORMATION in this way, or otherwise that such processing is lawful. Except in the event of CHASE'S gross negligence or fraud, YOU hereby indemnify and holds harmless CHASE, its directors, employees and/or contractors, now and in the future from any claim, expense, damages and legal costs arising from:**

1.22.1.1 **YOUR failure to obtain the third-party's consent to lawfully process their PERSONAL INFORMATION and/or SECONDARY INFORMATION;**

1.22.1.2 **YOUR breach of any relevant data protection legislation in the RSA, including POPI.**

1.22.2 You consent to CHASE retaining back-ups of YOUR PERSONAL INFORMATION and SECONDARY INFORMATION for no less than 8 (eight) years after termination of the CHASE AGREEMENT or for longer as may be

required in law for the retention of records. CHASE provides no warranty in respect of the effectiveness of such backups.

1.22.3 To the extent that YOU collect SECONDARY INFORMATION in terms of this EULA and/or the CHASE AGREEMENT when using the SOFTWARE as a responsible party in terms of POPI, YOU will be responsible for all obligations of a responsible party in terms of POPI.

1.22.4 YOU undertake to advise CHASE as soon as reasonably possible of if the Regulator investigates YOU or makes a ruling against YOU pertaining to YOUR failure or contravention of POPI.

1.22.5 When accessing, dealing with, collecting and/or processing PERSONAL INFORMATION and/or SECONDARY INFORMATION, using the SOFTWARE, YOU must at all times:

1.22.5.1 not request, collate, process and/or store PERSONAL INFORMATION and/or SECONDARY INFORMATION which is not necessary for the lawful purpose for which the PERSONAL INFORMATION and/or SECONDARY INFORMATION is required;

1.22.5.2 obtain written permission from the database subject for the collection, collation, processing and/or disclosure of any PERSONAL INFORMATION and/or SECONDARY INFORMATION;

1.22.5.3 not use the PERSONAL INFORMATION and/or SECONDARY INFORMATION for any purpose other than for the disclosed purpose for which the database subject gave their written permission;

1.22.5.4 keep a record of the PERSONAL INFORMATION and/or SECONDARY INFORMATION and the reason for which the PERSONAL INFORMATION and/or SECONDARY INFORMATION was collected, for as long as the PERSONAL INFORMATION and/or SECONDARY INFORMATION is used by YOU;

1.22.5.5 not disclose the PERSONAL INFORMATION and/or SECONDARY INFORMATION to any third-party, unless permitted by legislation to do so or authorised in writing by the database subject to do so. A record of any such disclosure must be kept for as long as the PERSONAL INFORMATION and/or SECONDARY INFORMATION is used by the database subject and the record must contain details on the reasons for the disclosure, the date of disclosure and the entity or person to whom disclosure was made;

1.22.5.6 delete and/or destroy any PERSONAL INFORMATION and/or SECONDARY INFORMATION that becomes obsolete. Prior written approval must be obtained from the database subject before any such deletion and/or destruction takes place; and

1.22.5.7 treat all PERSONAL INFORMATION and/or SECONDARY INFORMATION in a consistent and confidential manner.