## 1 Purpose and scope

1.1 Our privacy policy governs how we collect, handle, use and disclose your personal information. It provides guidelines to ensure that the personal information about individuals collected and held by Entyce Food Ingredients Pty Ltd ("**Entyce**") is kept secure and that the privacy obligations of Entyce are applied consistently across Entyce's business.

1.2 This Policy, therefore, sets out the types of personal information that we may collect and hold, how that information is used and with whom the information is shared. It also deals with how you can access the personal information we hold about you, ask us to correct it, or make a privacy related complaint. This policy explains how we respect your right to privacy in accordance with the Australian Privacy Principles ("**APPs**") contained in the *Privacy Act 1988* (Cth) ("**Privacy Act**"). The APPs are designed to protect the confidentiality of information and the privacy of individuals by regulating the way personal information is collected, used, disclosed and managed.

## 2 Definitions

2.1 **Personal information:** When this policy refers to personal information it is a reference to personal information as defined in the Privacy Act. Personal information is, generally speaking, information or an opinion relating to an identified, or reasonably identifiable, individual, whether the information is true or not and regardless of whether Entyce has kept a record of it.

2.2 **Entyce IT Facilities:** Means Entyce's computers, software, hardware, the internet, email, instant messaging, telephones and Mobile Devices, computer and information systems, networks and infrastructure (including local and shared drives) of Entyce.

2.3 **Mobile Device:** Any portable device that is capable of capturing, storing, transmitting or displaying data; including: laptops, tablets, mobile data storage devices and mobile phones that are connected to or have access to the Entyce office wireless network or virtual private network (VPN) or Entyce web-based email. For the avoidance of doubt, this includes both devices owned by Entyce, and your own devices used for work purposes.

2.4 **Sensitive information:** When this policy refers to sensitive information it is a reference to sensitive information as defined under the Privacy Act, which includes information about an individual's health, racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association or membership of a trade union. For Entyce, it will include health information and biometric information that is to be used for the purpose of automated biometric verification or biometric identification.

2.5 **Computer Surveillance:** Is surveillance by means of software or other equipment that monitors or records the information input or output, or other use, of Entyce's IT Facilities (including, but not limited to the use of a computer, laptop, tablet, smart phone, and including the sending and receipt of emails and messages, and the accessing of websites).

## 3 What kind of Information does Entyce Collect and Hold?

3.1 Entyce may collect personal and sensitive information that is reasonably necessary to be collected for the purposes of Entyce fulfilling its functions and activities.

3.2 Entyce may ask for identification information. This information may include but is not limited to an individual's name, address, contact details, date of birth, and tax file number.

However, we will not use identifiers assigned by the Government, such as a tax file number, Medicare number or provider number, for our own file recording purposes.

3.3 Entyce may collect and hold personal information, such as, but not limited to, names of employees and proprietors of organisations, addresses, telephone numbers, facsimile numbers, e-mail addresses, titles, professional affiliations, and financial information such as your bank details. For those who work at, or seek to work at Entyce, this may also include information about your qualifications and employment history.

3.4 Entyce may collect sensitive information (including health information) such as any vulnerability you may have. When we request your sensitive information, we will identify which information is necessary and which information may be provided with your consent. If you choose not to supply any of the information we request, our ability to assist you may be limited.

3.5 For visitors to any of our premises, Entyce may require, in addition to all other identification information, that an individual provide certain biometric information to allow automatic registration of entry, departure and movement within our sites, and may obtain and record other information such as temperature and vaccination status.

3.6 Entyce may collect and hold additional personal information about individuals. This could include visitors, transaction information or making a record of queries or complaints an individual makes and, if they make an insurance claim, collecting additional information to assess the claim.

## 4 How and Why does Entyce Collect and Hold this Information?

4.1 Entyce will collect personal information in a number of ways, including information provided directly from you, provided by our agents, contractors or distributors, or provided through our website. We can collect this information by way of emails, via telephone calls (which may be recorded for quality control purposes in accordance with applicable laws), in person from any visitor to our sites, from video conferencing, face-to-face meetings and interviews, from any application you make (in whatever format) to become an Entyce customer, supplier, employee or contractor, when you provide feedback to us, submit an enquiry, respond to a promotion by submitting your details, participate in a survey or competition, when you create an account with us, purchase a product or service from us, and when we otherwise do business with you or when you provide services to us or visit any of our offices and sites.

4.2 We collect personal information for a number of purposes connected with our activities and operations, including, but not limited to:

4.3 conducting our business, providing Entyce products and services to customers and clients, and selling and marketing of our products and extended range of services;

4.4 complying with statutory and other legal requirements, including but not limited to taxation, occupational health and safety, industrial law and health regulations;

4.5 ensuring the integrity and security of Entyce premises as a secure food production site;

4.6 for verification purposes, and to understand and meet the needs and requests of individuals with whom we engage;

4.7 managing our business relationships;

4.8 completing a transaction on your behalf;

4.9 developing, providing and improving our products and services;

4.10 providing information about our products and services; and

4.11 for our internal administrative, planning, product development and research requirements.

4.12 From time to time, we may use your contact details to send you direct marketing communications including offers, updates and newsletters that are relevant to the services we provide. We may do so by mail or electronically unless you tell us that you do not wish to receive electronic communications. We always give you the option of electing not to receive these communications in the future. You can unsubscribe by notifying us and we will no longer send this information to you.

4.13 Entyce will not collect any personal information except when the individual has knowingly provided that information to us or authorised a third party to provide that information to us.

## 5 Keeping Information Secure

5.1 Entyce uses security procedures and technology to protect the information we hold. To prevent misuse or unlawful disclosure of sensitive information, Entyce has implemented internal policies which cover staff conduct, continuous training and monitoring of staff, and the inclusion of checks in the Audit function. If other organisations provide support services, we require these organisations to appropriately safeguard the privacy of the information provided to them.

5.2 Where the personal information we collect is no longer required, we will delete the information or permanently de-identify it in accordance with relevant laws and our internal records management policy.

5.3 For visitors to an Entyce site that may have biometric identification points in place, please note that there are additional safeguards in place, which can be found under Part 8 below.

## 6 Accessing and correction of Personal Information

6.1 Entyce will take reasonable steps to ensure that the personal information that it collects is accurate, up-to-date and complete.

6.2 We take all reasonable steps to protect your personal information from misuse, interference, loss, unauthorised access, modification or exposure. All employees, directors and contractors are required by the terms of their contract to maintain the confidentiality of information. Access to your information is restricted to those employees whose job requires that information. Access to our premises and computer systems is restricted through locks, password protection, internet firewalls and routers.

6.3 Entyce does not sell, trade or rent lists of personal information to any third party. In all cases we will only disclose that information that is strictly required and take all reasonable steps to ensure that your personal information is handled in accordance with the APPs.

6.4 Otherwise, we will not disclose personal information unless you consent, we are required to do so by law or under some unusual other circumstances which the Privacy Act permits.

6.5 Under the Privacy Act, individuals have a right to seek access to information which we hold about them; although, there are some exceptions to this. They also have the right to ask us to correct information about them, which is inaccurate, incomplete or out of date. To do so, they must contact Entyce.

6.6 We do not charge for receiving a request for access to personal information or for complying with a correction request. We do however reserve the right to charge you for all reasonable costs and outgoings specifically incurred in meeting your request for information. In processing an individual's request for access to their personal information, a reasonable cost may be charged if they have requested access more than once within twelve months. This charge covers such things as locating the information and supplying it to them.

6.7 There are some circumstances in which Entyce are not required to give individuals access to their personal information. If Entyce refuse to give an individual access to or to correct their personal information, Entyce will give them a notice explaining the reasons why, except

where it would be unreasonable to do so. If we refuse an individual request to correct their personal information, the individual also has the right to request that a statement be associated with their personal information noting that they disagree with its accuracy. If Entyce refuses an individual's request to access or correct their personal information, we will also provide them with information on how they can complain about the refusal.

## 7 Notification

7.1 Due to the *Privacy Amendment (Notifiable Data Breaches) Act 2017*, Entyce is legally required to notify affected individuals of any eligible data breaches. To comply with this legal requirement, Entyce has implemented a Data Breach Response Plan in order to deal with actual or potential data breaches as well as the notification process to be followed when notifying affected individuals.

## 8 Specific Protections for Biometric Data

8.1 We recognise that our biometric sign-in technology will collect sensitive information which is may be used at our offices and site locations. Entyce will collect and use and disclose your sensitive information only for the primary purpose for which it was collected, or for directly related purposes which would reasonably be expected by you, or for purposes to which you have consented and in other circumstances required or authorised by law.

8.2 To ensure proper data protection and privacy for your sensitive information, we have partnered with Noah Face and Wage Loch to implement and launch our biometric sign-in and temperature measuring technology for visitors, staff and contractors. These technology providers have worked with many reputable Australian companies to implement similar systems in their workplaces. They will collect and process the data on our behalf, and we have been advised that the data will be stored at their respective hosting facilities in Australia.

8.3 Moreover, the data will only be retained by Noah Face and Wage Loch for as long as Entyce determines, and Entyce controls when it is deleted.

8.4 For further information, please read Noah Face's data protection policy here and privacy policy here or at their website: www.noahface.com

8.5 For further information, please read Wage Loch's privacy policy here or website: www.wageloch.com.au

## 9 What happens if I have concerns about privacy?

9.1 If you have concerns about whether we have complied with the Privacy Act or this privacy policy, please contact our Technical & Operations Manager Ms. Sandra Ciantar by email at sandra@entyce.com.au or on 03 8203 2032. Your complaint will be considered through our internal complaint's resolution process, and we will try to respond with a decision quickly and promptly, aiming to respond no later than within 45 days of you making the complaint.

## 10 Your consent

10.1 By using the Entyce Website, our Store, or an Entyce's product, service, application and/or site that references this Privacy Policy, or otherwise providing us directly, or through others, with your personal information, including physical attendance at any of our office or factory locations, you agree with the terms of this Privacy Policy and consent to the collection, use, and disclosure of that information in accordance with this Privacy Policy, the Privacy Act and other applicable privacy laws.