

**Hypertech Protection Services Pty Ltd t/a Hypertech Security - Privacy Policy****1. OUTLINE**

**1.1 Scope.** This Privacy Policy, which is subject to the Privacy Act and APPs, regulates how we collect, use and disclose *personal information*.

**1.2 Amendment.** We may change, vary or modify all or part of this Privacy Policy at any time in our sole discretion. It is your responsibility to check this Privacy Policy periodically for changes. If we adopt a new Privacy Policy:

1.2.1 we will post the new Privacy Policy on our Platforms; and

1.2.2 it will then apply through your acceptance of it by  
subsequent or continued use of our Platforms and/or our  
Products or Services.

**1.3 Employee records.** This Privacy Policy does not apply to our acts and practices which relate directly to the employee records of our current and former employees.

**1.4 Other policies.** To the extent possible, Hypertech Security and its Related Bodies Corporate have adopted a uniform approach to collecting, using, disclosing and protecting *personal information*.

**2. PURPOSE****2.1 Primary and Secondary Purposes for collection.**

We collect *personal information* from you and, subject to clause 3.3, you consent to us

using your *personal information* (other than *sensitive information*) for the following Primary and Secondary Purposes:

| Purpose/Activity   | Type of <i>personal information</i>   | Basis for use   |
|--|---|---|
| <b>Products and Services</b><br>To process and deliver Products and Services requested by you, including but not limited to: <ul style="list-style-type: none"> <li>· preparing and delivering documents;</li> <li>· managing payments, fees and charges;</li> <li>· collecting and recovering money owed to us; and</li> <li>· verifying your identity</li> </ul> | <ul style="list-style-type: none"> <li>· Identity</li> <li>· Contact</li> <li>· Financial</li> <li>· Transaction</li> <li>· Client</li> </ul>                                     | <ul style="list-style-type: none"> <li>· Performance of a contract with you</li> <li>· Legal and regulatory requirement</li> <li>· Necessary for our legitimate interests (e.g. to recover debts due to us)</li> </ul>  |
| <b>Information</b><br>To provide you with information about the Products or Services you requested and any other products or services which we consider you may be interested in   | <ul style="list-style-type: none"> <li>· Identity</li> <li>· Contact</li> <li>· Client</li> <li>· Marketing and Communications</li> </ul>   | <ul style="list-style-type: none"> <li>· Performance of a contract with you</li> <li>· Improvement of delivery of Products and Services to you</li> </ul>   |
| <b>Customer experience</b><br>To personalise and customise your experiences with us  | <ul style="list-style-type: none"> <li>· Identity</li> <li>· Contact</li> <li>· Client</li> <li>· Technical</li> <li>· Marketing and Communications</li> <li>· Profile</li> </ul> | <ul style="list-style-type: none"> <li>· Performance of a contract with you</li> <li>· Improvement of delivery of Products and Services to you</li> </ul>   |
| <b>Business Development</b><br>To help us review, manage or enhance our Products or Services, and develop insights which may be used in reports or other content developed by us   | <ul style="list-style-type: none"> <li>· Identity</li> <li>· Contact</li> <li>· Client</li> <li>· Technical</li> <li>· Marketing and Communications</li> <li>· Profile</li> </ul> | <ul style="list-style-type: none"> <li>· Necessary for our legitimate interests (e.g. to study how our customers interact with and use our Products and Services, to develop our Products and Services, to grow our business, and to inform our marketing strategy)</li> </ul>      |
| <b>Communications</b><br>To communicate with you, including by email, mobile and in-application notifications  | <ul style="list-style-type: none"> <li>· Identity</li> <li>· Contact</li> <li>· Profile</li> </ul>  | <ul style="list-style-type: none"> <li>· Performance of a contract with you</li> <li>· Necessary for our legitimate interests (e.g. to resolve any matters that require additional services or attention by us in relation to the Products or Services delivered to you)</li> </ul> |
| <b>Surveys and promotions</b><br>To conduct surveys or   | <ul style="list-style-type: none"> <li>· Identity</li> <li>· Contact</li> </ul>   | <ul style="list-style-type: none"> <li>· Necessary for our legitimate interests (e.g. to study how our customers</li> </ul>   |

| <b>Purpose/Activity</b>  | <b>Type of <i>personal information</i></b>   | <b>Basis for use</b>   |
|--|--|--|
| promotions   | <ul style="list-style-type: none"> <li>· Client</li> <li>· Marketing and Communications</li> <li>· Profile</li> </ul>  | <ul style="list-style-type: none"> <li>· Interact with and use our Products and Services, to develop our Products and Services, to grow our business, and to inform our marketing strategy)</li> <li>· Improvement of delivery of Products and Services to you</li> </ul>  |
| <b>Payments and Accounts</b><br>To process payments and administer your account, including to send you account related reminders   | <ul style="list-style-type: none"> <li>· Identity</li> <li>· Contact</li> <li>· Financial</li> <li>· Transaction</li> <li>· Client</li> </ul>  | <ul style="list-style-type: none"> <li>· Legal and regulatory requirement</li> <li>· Necessary for our legitimate interests (e.g. to recover debts due to us)</li> </ul>   |
| <b>Complaints</b><br>To investigate any complaints about or made by you, or if we have reason to suspect you have breached any relevant terms  | <ul style="list-style-type: none"> <li>· Identity</li> <li>· Contact</li> <li>· Financial</li> <li>· Transaction</li> <li>· Client</li> </ul>  | <ul style="list-style-type: none"> <li>· Legal and regulatory requirement</li> <li>· Necessary for our legitimate interests (e.g. to ensure that we continue to deliver Products and Services in accordance with industry best-practice)</li> </ul>  |
| <b>Service Providers and Partners</b><br>To work with commercial and technology partners as well as affiliates of repute (whether for profit, economic benefit or otherwise) so that data collected by us and/or them on our behalf may be used by those third parties for commercial, analytic, service provision and/or communication purposes (or otherwise on a basis contemplated by this document) | <ul style="list-style-type: none"> <li>· Identity</li> <li>· Contact</li> <li>· Transaction</li> <li>· Client</li> <li>· Technical</li> <li>· Marketing and Communications</li> <li>· Profile</li> </ul> | <ul style="list-style-type: none"> <li>· Enables us to provide third parties with personal information and data so that commercial opportunities and goods and/or services of interest may be offered to you</li> <li>· Enables technology partners to provide us and you with facilitative technology services of relevance to the digital economy</li> <li>· Necessary for our legitimate interests (e.g. to encourage our business and revenue growth)</li> </ul> |
| <b>Receiving Services</b><br>To receive services from you or the organisation which employs you  | <ul style="list-style-type: none"> <li>· Transaction</li> <li>· Client</li> </ul>  | <ul style="list-style-type: none"> <li>· Performance of a contract with you</li> <li>· Necessary for our legitimate interests</li> </ul>   |
| <b>Employment</b><br>To help us assess an application submitted by you or on your behalf in relation to your employment  | <ul style="list-style-type: none"> <li>· Identity</li> <li>· Contact</li> <li>· Client</li> <li>· Technical</li> <li>· Profile</li> <li>· Financial</li> </ul>   | <ul style="list-style-type: none"> <li>· Performance of a contract with you</li> <li>· Legal and regulatory requirement</li> <li>· Necessary for our legitimate interests (e.g. to determine your suitability for employment with us)</li> <li>· Arranging for payment to you in accordance with your employment contract</li> </ul>   |
| <b>General Business and Legal Obligations</b>  | <ul style="list-style-type: none"> <li>· Identity</li> <li>· Contact</li> </ul>  | <ul style="list-style-type: none"> <li>· Legal and regulatory requirement</li> <li>· Necessary for our legitimate interests</li> </ul>   |

| Purpose/Activity  | Type of <i>personal information</i>  | Basis for use   |
|---|--|---|
| To lawfully carry out our functions and activities and do anything else as required or permitted by any law | <ul style="list-style-type: none"> <li>· Financial</li> <li>· Transaction</li> <li>· Client</li> <li>· Technical</li> <li>· Marketing and Communications</li> <li>· Profile</li> </ul> | · Improvement of delivery of Products and Services to you |

### 3. WHAT WE COLLECT

**3.1 Personal Information.** *Personal information* we collect about you may include identification information such as your name, position, address, email address, date of birth, gender, driver's licence number, mobile phone number, business references, details about your business, Australian Business Number, insurance details, rates and fees, your occupation, career history and references, financial and payment information (including credit card and banking information) and such other information necessary or convenient for delivering our Products and Services. We also may collect additional information as part of our collection of Identity, Contact, Financial, Transaction, Technical, Marketing and Communications, Client and Profile information used for the Primary and Secondary Purposes.

**3.2 Other information.** We may collect, and you consent to us collecting, information relating to you that is not *personal information*, such as data relating to your activity on our Platforms, including:

- 3.2.1 the Internet Protocol address and a component of the domain name used (e.g. .com or .net);
- 3.2.2 the type of browser and operating system you used;
- 3.2.3 the date and time you visited our Platforms;
- 3.2.4 the web pages or services you accessed at our Website;
- 3.2.5 the time spent on individual pages and our Website overall;
- 3.2.6 which files you downloaded; and
- 3.2.7 information about your computer and Internet connections using cookies.

**3.3 Sensitive Information.** We will only collect, hold, use or disclose your *sensitive information* with your consent or if you volunteer your *sensitive information* to us. If we collect or hold your *sensitive information* in accordance with this clause, we may disclose such *sensitive information* to our Related Bodies Corporate. However neither us nor our Related Bodies Corporate may use or disclose your *sensitive information* to any Third Party except as required or permitted by law.

## 4. HOW WE COLLECT

**4.1 How we collect.** Your *personal information* may be collected:

- 4.1.1 when you complete an application, consent, purchase, account sign-up or similar form via our Platforms or otherwise;
- 4.1.2 when you register for an event or webinar or provide us with your business card;
- 4.1.3 when you contact us to submit a query or request (whether in writing, verbally, in hardcopy or electronic format);
- 4.1.4 when you contact us by telephone, mail, email, fax or face-to-face;
- 4.1.5 when you post information or otherwise interact with the Platforms;
- 4.1.6 when you participate in one of our competitions or surveys;
- 4.1.7 from those who request our Products or Services on your behalf;
- 4.1.8 from publicly available sources of information;
- 4.1.9 from government regulators, law enforcement agencies;
- 4.1.10 when you complete an application for employment with us;
- 4.1.11 when negotiating or entering into a contracting relationship with us;
- 4.1.12 from business contacts, external service and supply providers and; or
- 4.1.13 by other means reasonably necessary.

**4.2 Third party collection.** Where possible, we collect your *personal information* directly from you. If we collect any *personal information* about you from someone other than you, to the extent not already set out in this Privacy Policy, we will

inform you of the fact that we will collect, or have collected, such information and the circumstances of that collection before, at or as soon as reasonably practicable after we collect such *personal information*.

**4.3 Authority.** If you provide us with the *personal information* of another individual, without limiting any other provision of this Privacy Policy, you acknowledge and agree that the other individual:

- 4.3.1 has authorised you to provide their *personal information* to us  
(and you have provided them with a copy of this Privacy Policy; and
- 4.3.2 consents to us using their *personal information* in order for  
us to provide our Products and Services.

**4.4 Unsolicited information.** If we receive unsolicited *personal information* about you that we could not have collected in accordance with this Privacy Policy and the Privacy Act, we will, within a reasonable period, destroy or de-identify such information received.

**4.5 Anonymity.** If you would like to access any of our Products and Services on an anonymous or pseudonymous basis we will take reasonable steps to comply with your request, however:

- 4.5.1 you may be precluded from taking advantage of some or all  
of our Products and Services; and
- 4.5.2 we will require you to identify yourself if:
  - a) we are required by law to deal with individuals who have  
identified themselves; or
  - b) it is impracticable for us to deal with you if you do not  
identify yourself.

**4.6 Destruction.** Subject to a legal requirement to the contrary, we will destroy or de-identify within 5 days your *personal information* if:

- 4.6.1 the purpose for which we collected the *personal information* from you no longer exists or applies; or
- 4.6.2 you request us to destroy your *personal information*, and we are not required by law to retain your personal information.

**4.7 Website and Google Analytics.** Information we collect may include:

- 4.7.1 the Internet Protocol address and a component of the domain name used (e.g. .com or .net);
- 4.7.2 the type of browser and operating system you used;
- 4.7.3 the date and time you visited our Platform(s);
- 4.7.4 the web pages or services you accessed on our Platform(s);
- 4.7.5 the time spent on individual pages and our Platform(s) overall;
- 4.7.6 which files you downloaded; and
- 4.7.7 information about your computer and Internet connections using cookies (see clause 4.8 below).

We may have integrated Google Analytics into the Platforms (see <http://www.google.com/analytics/> for details). We use Google Analytics Demographics and Interest Reports to obtain a more detailed understanding of our Platforms users and their potential needs. Data collected from such reports may be used to more accurately target marketing and advertising campaigns based on demographic information and more generally for the Primary Purposes and Secondary Purposes detailed in this Privacy Policy. We do not collect *personal information* about individuals by such methods; only aggregate data is collected and used for planning purposes.

**4.8** We may use 'cookie' technology to assist us to determine in the aggregate the total number of visitors to the Platforms on an ongoing basis and the types of internet browsers and operating systems used by users of the Platforms. This information is used to enhance the usability and functionality of our Platforms and for marketing, advertising and analytic purposes.

## 5 USE

**5.1 Primary use.** We will only use and disclose your *personal information*:

5.1.1 for purposes which are related to the Primary and Secondary Purposes; or

5.1.2 if we otherwise get your consent to do so,  
in accordance with this Privacy Policy and the Privacy Act.

**5.2 Reasonable uses.** We will not use your *personal information* for any purpose for which you would not reasonably expect us to use your *personal information*.

**5.3 Third parties.** You consent to us providing your *personal information* (other than *sensitive information*) to commercial and technology partners as well as affiliates of repute and our Related Bodies Corporate. We may do so for profit or economic benefit and this may include (without limitation) licence arrangements and rights of use in relation to or in connection with direct marketing, analysis, data aggregation and anything else reasonably required or permitted by law. Data collected by us and/or them on our behalf may be used by those third parties for commercial, analytic, service provision and/or communication purposes (or otherwise on a basis contemplated by this document). The provision of such *personal information* to Third Parties and Related Bodies Corporate may be subject to the relevant privacy policies of such third persons.

**5.4 Direct marketing.** We may deliver direct marketing communications to you about our Products and Services and any other products or services you might be interested in. If you notify us that you do not want to receive these communications, we will comply with your instruction and will not use your *personal information* for this purpose.

**5.5 Right to use.** Subject to any other term of this Privacy Policy, we will only use or disclose your *personal information* for the purposes of direct marketing if:

5.5.1 we collected the information from you;

5.5.2 it is reasonable in the circumstances to expect that we would use or disclose

the information for direct marketing purpose;

5.5.3 we provide you with a simple means to 'opt-out' of direct marketing from us;

5.5.4 you have not elected to 'opt-out' from receiving such direct marketing

**5.6 Opt-out.** You may opt-out of receiving direct marketing communications by:

5.6.1 contacting us using our contact details set out at clause 10.

## **6. DISCLOSURE**

**6.1. How we disclose.** We may disclose *personal information* and you consent to us disclosing such *personal information* (other than *sensitive information*) for purposes which are related to the Primary and Secondary Purposes, or as otherwise set out in this Privacy Policy, including but not limited to:

6.1.1 Third Parties engaged by us to perform functions or provide Products or Services on our behalf;

6.1.2 Third Parties that engage us to provide Products or Services to them;

6.1.3 Third Parties who assist us with a number of our functions and services including but not limited to service providers of technology, data processing, market research, mail outs, marketing and advertising, but only for the purpose of fulfilling those services;

6.1.4 your referees and former employees (in relation to employment applications only);

6.1.5 credit agencies;

6.1.6 relevant regulatory bodies in the industry in which we or you operate;

6.1.7 our professional advisors, including our accountants, auditors and lawyers;

6.1.8 our related bodies corporate;

6.1.9 persons authorised by you to receive information held by us, which for the avoidance of doubt includes but is not limited to our business partners that we may have commercial arrangements with from time to time including Third Parties who we contract with for our independent commercial purposes;

6.1.10 a government authority, law enforcement agency, pursuant to a court order or as otherwise required by law;

6.1.11 a party to a transaction involving the sale of our business or its assets

**6.2** (future)

**6.3 Non-identifiable information.** We may share non-personally identifiable information publicly and with our partners (e.g. relevant Third Party suppliers or service providers, publishers, advertisers, sponsors, or connected sites). For example, we may share information publicly to show trends about the general use of our Products and/or Services.

**6.4 Overseas disclosure.** We may in some circumstances as necessary send your *personal information* to overseas recipients to enable us provide our Products or Services to you. The countries in which likely overseas recipients of *personal information* are located includes: USA, Germany, Korea and China.

**6.5 Overseas recipients.** Overseas recipients that may handle or process your data include (but are not limited to) persons the server hosts of our email services, cloud storage services and the Platforms.

**6.6 Reasonable protections.** If we send your *personal information* to overseas recipients, we will take reasonable measures to protect your *personal information* from misuse, interference, loss, unauthorised access or modification. However, you acknowledge and agree that if we disclose your *personal information* to overseas recipients, we are not obliged to take reasonable steps to ensure overseas recipients of your *personal information* comply with the Privacy Act and the APPs.

**6.7 GDPR.** If we become aware that you are a citizen of, or are located within, the European Union at the time when we collect *personal information* about you, or at the time when we propose to transfer *personal information* about you overseas, we will take steps to ensure (to the extent relevant) that we comply with Articles 45 to 49 of the

GDPR in relation to the transfer of your *personal information* overseas. However, you acknowledge that as we conduct our business from and predominantly within Australia, you are required to provide us with written notice of our need to comply with the European General Data Protection Regulation in relation to your *personal information* if you wish for us to take steps that are not already set out in this Privacy Policy.

## **7. ACCESS+CORRECTION**

**7.1 Access.** If you require access to your *personal information*, please contact us using our contact details set out at clause 10. You may be required to put your request in writing and provide proof of identity.

**7.2 Exceptions.** We are not obliged to allow access to your *personal information* if:

7.2.1 it would pose a serious threat to the life, health or safety of any individual or to the public;

7.2.2 it would have an unreasonable impact on the privacy of other individuals;

7.2.3 the request for access is frivolous or vexatious;

7.2.4 it relates to existing or anticipated legal proceedings between you and us and would not ordinarily be accessible by the discovery process in such proceedings;

7.2.5 it would reveal our intentions in relation to negotiations with you in a way that would prejudice those negotiations;

7.2.6 it would be unlawful;

7.2.7 denying access is required or authorised by or under an Australian law or a court/tribunal order;

7.2.8 we have reason to suspect that unlawful activity, or misconduct of a serious nature relating to our functions or activities has been, is being or may be engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter;

7.2.9 it would likely prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body;

7.2.10 it would reveal commercially sensitive information; or

7.2.11 a relevant law provides that we are not obliged to allow access to

your *personal information* (e.g. the GDPR).

**7.3 Response to access request.** If you make a request for access to *personal information*, we will:

7.3.1 respond to your request within a reasonable period after the request is made; and

7.3.2 if reasonable and practicable, give access to the personal information as requested.

**7.4 Refusal of access.** If we refuse to give access to the *personal information*, we will give you a written notice that sets out at a minimum:

7.4.1 our reasons for the refusal (to the extent it is reasonable to do so); and

7.4.2 the mechanisms available to complain about the refusal.

**7.5 Correction.** We request that you keep your *personal information* as current as possible. If you feel that information about you is not accurate or your details have or are about to change, you can contact us using our contact details set out at clause 10.

**7.6 Response to correction request.** If you make a request for us to correct your *personal information*, we will:

7.6.1 respond to your request within a reasonable period after the request is made; and

7.6.2 if reasonable and practicable, correct the information as requested.

**7.7 Refusal to correct.** If we refuse a request to correct *personal information*, we will:

7.7.1 give you a written notice setting out the reasons for the refusal and how you may make a complaint; and

7.7.2 take reasonable steps to include a note with your *personal information* of the fact that we refused to correct it.

**7.8 EU Restriction.** If you are a citizen of, or are located within, the European Union at the time at which we collect personal data about you, or at the time at which you make a relevant request, we will take steps to ensure that we comply with a request by you to restrict our use of your personal data pursuant to Article 18 of the GDPR. You acknowledge that, depending on the nature of the restriction you request, we may be unable to provide you with some or all of our Products or Services (or any part of any Product or Service) if we comply with your request. In such circumstances, we will advise you of our inability to provide or continue to provide you with the relevant Products or Services, and if you confirm that you would like us to comply with your request, we may terminate a relevant agreement or other document with you in relation to our Products or Services.

## **8. SECURITY + PROTECTION**

**8.1 Reasonable protections.** In relation to all *personal information*, we will take all reasonable steps to:

8.1.1 ensure that the *personal information* we collect is accurate, up to date and complete;

8.1.2 ensure that the *personal information* we hold, use or disclose is, with regard to the relevant purpose, accurate, up to date, complete and relevant; and

8.1.3 protect *personal information* from misuse, loss or unauthorised access and disclosure.

**8.2 Security.** We require staff and service providers to respect the confidentiality of *personal information*. We store your *personal information* in an access controlled building with intruder alarm and CCTV coverage on a secure server behind a firewall and use security software accessible only by authorised personnel and service providers to protect your *personal information* from unauthorized access, destruction, use, modification or disclosure.

All employee/contractor Smart Phones shall employ Password Control to lock their use.

**8.3 Obligation to notify.** You must contact us immediately if you become aware of or suspect any misuse or loss of your *personal information*.

## **9. COMPLAINTS**

**9.1 Complaint.** If you have a complaint about how we collect, use, disclose, manage or protect your *personal information*, or consider that we have breached the Privacy Act or APPs, please contact us using our contact details set out at clause 10. We will respond to your complaint within 14 days of receiving the complaint.

**9.2 Response and resolution.** Once the complaint has been received, we may resolve the matter in a number of ways:

**9.2.1 Request for further information:** We may request further information from you. Please provide us with as much information as possible, including details of any relevant dates and documentation. This will enable us to investigate the complaint and determine an appropriate solution.

**9.2.2 Discuss options:** We will discuss options for resolution with you and if you have suggestions about how the matter might be resolved you should raise these with our Privacy Officer.

**9.2.3 Investigation:** Where necessary, the complaint will be investigated. We will try to do so within a reasonable time frame. It may be necessary to contact others in order to proceed with the investigation. This may be necessary in order to progress your complaint.

**9.2.4 Conduct of our employees:** If your complaint involves the conduct of our employees we will raise the matter with the employees concerned and seek their comment and input in the resolution of the complaint.

**9.3 Notice of decision.** After investigating the complaint, we will give you a written notice about our decision.

**9.4 OAIC.** You are free to lodge a complaint directly with the OAIC online, by mail, fax or email. For more information please visit the OAIC website at *oaic.gov.au*.

## **10. CONTACT**

10.1 Please forward all correspondence in respect of this Privacy Policy to:

Personal Information & Information Security Manager  
Hypertech Security  
PO Box 382  
Winston Hills NSW 2153  
Australia  
P: 02 9631 1008  
E: [info@hypertech.com.au](mailto:info@hypertech.com.au)

## **11. INTERPRETATION + DEFINITIONS**

11.1 **Personal pronouns.** Except where the context otherwise provides or requires:

11.1.1 the terms **Hypertech Security**, **we**, **us** or **our** refers to Hypertech Protection Services Pty Ltd (ABN 16 084 642 866); and

11.1.2 the terms **you** or **your** refers to a user of the Platform and/or a customer to whom we provide the Products or Services or from whom we collect personal information or data.

**7.2 Italicised terms.** Terms italicised and defined in the Privacy Act have the meaning given to them in the Privacy Act.

**7.3 Defined terms.** In this Privacy Policy unless otherwise provided, the following terms shall have their meaning as specified:

**APPs** means any of the Australian Privacy Principles set out in Schedule 1 of the Privacy Act.

**Client information** includes information about how you use the Products or Services or our website, as well as *personal information* which can include Identity information, Contact information, Financial information, Transaction information and Profile information of you and/or your family members, beneficiaries, employees or employers, or other third persons about whom we need to collect *personal information* by law, or under the terms of a contract we have with you.

**Contact information** includes billing address, postal address, email address and telephone numbers (these details may relate to your work or to you personally, depending on the nature of our relationship with you or the company that you work for).

**Financial information** includes bank account, credit card, banking information and other payment method details, reasonably required details about your business such as Australian Business Number, insurance details, business references.

**GDPR** means *Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27<sup>th</sup>, 2016* (most commonly referred to as the General Data Protection Regulation or GDPR).

**Identity information** includes first name, maiden name, last name, username or similar identifier, marital status, title, date of birth, gender, your driver's licence number, job function and position, your employer or department.

**Marketing and Communications information** includes your preferences in receiving marketing from us and your communication preferences. This may include information about events to which you or your colleagues are invited, and your *personal information* and preferences to the extent that this information is relevant to organising and managing those events (for example, your dietary requirements).

**Platforms** means all or any of the relevant platforms, electronic interfaces (including the Products) and websites that are owned, provided and/or operated from time to time by us (including but not limited to the Website), regardless of how those interfaces and websites are accessed by users (including via the internet, mobile phone, mobile applications or any other device or other means).

**Primary and Secondary Purposes** means the primary and secondary purposes stated at clause 2.1.

**Privacy Act** means the *Privacy Act 1988* (Cth) as amended from time to time.

**Privacy Policy** means this privacy policy as amended from time to time.

**Profile information** includes your username and password, your interests, preferences, feedback, survey responses and all other information you provide through your use of the Products or Services, or otherwise through your contact or correspondence with us.

**Products** means products that we provide or offer from time to time.

**Related Bodies Corporate** has the meaning given to that term in the *Corporations Act 2001* (Cth) and in the case of Hypertech Security includes any entity in which Hypertech Security has (directly or indirectly) an equity stake of 10% or more, or has a services agreement under which any such person is required to provide for the benefit of the other entity services or deliverables; or is connected to or operates under a brand or trademark (owned or under licence) of Hypertech Security or persons in which such a stake is held.

**Services** means our membership and business services such as consulting, advocacy, training, employment and industrial relations services, international trade services, apprenticeship and traineeship services, labour hire services, general business products and services provided through our various divisions and Related Bodies Corporate, and any other products or services offered or performed by us from time to time.

**Technical information** includes (as relevant):

(a) The Internet protocol (IP) address used to connect your computer to the Internet, your login information, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform;

(b) Information about your visit to our website/Products, such as the full Uniform Resource Locators (URL), clickstream to, through and from our website/Products (including date and time), services viewed or searched for, page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), methods used to browse away from a page, any phone number used to call our central switchboard number, and direct dials or social media handles used to connect with our fee earners or other employees; and

(c) Location data which we may collect through our website/Products and which provides your real-time location in order to provide location services (where requested or agreed to by you) to deliver content or other services that are dependent on knowing where you are. This information may also be collected in combination with an identifier associated with your device to enable us to recognise your mobile browser or device when you return to the website/App. Delivery of location services will involve reference to one or more of the following:

(i) the coordinates (latitude/longitude) of your location;

(ii) look-up of your country of location by reference to your IP address against public sources; and/or

(iii) your Identifier for Advertisers (IFA) code for your Apple device, or the Android ID for your Android device, or a similar device identifier. See our cookie policy for more information on the use of cookies and device identifiers on the website/Apps.

**Third Party** means any party that is not us or one of our Related Bodies Corporate.

**Transaction information** includes details about payments to and from you and other associated information.

**Website** means *www.hypertech.com.au* and that of its Related Bodies Corporate and all relevant sub-domains.



**Data Protection Impact Assessment (DPIA) relating to:**  
**[HYPERTECH SECURITY – CONSENT TO DISCLOSURE OF PERSONAL INFORMATION FORM]**

DPIAs should be sent to the Personal Information & Information Security Manager [info@hypertech.com.au](mailto:info@hypertech.com.au)

---

**Document control**

| Version | Date      | Author      | Summary of changes          | Approver | Approval date |
|---------|-----------|-------------|-----------------------------|----------|---------------|
| 1       | 31.1.2020 | Mark Gordon | Initial Assessment Document | MG       | January 2020  |
|         |           |             |                             |          |               |
|         |           |             |                             |          |               |
|         |           |             |                             |          |               |
|         |           |             |                             |          |               |

### Part A: Summary of the Initiative

**Describe the scope of the Initiative** (to include its aims and objectives; business/research/other case; level of investment in terms of time, financial and other resources; duration and geographic reach; visibility within and outside the organisation)

The scope of this initiative is to obtain personal information from our clients, client family members and or clients staff, and Hypertech Security to forward the relevant information to Back to Base Alarm Monitoring Centres, Guard Services, Strata Managers to allow these agencies to contact the client/client family members, client staff in the case of intrusion alarms etc being received or processed by these agencies

**Status of the Initiative** (describe the current phase of development or implementation of the Initiative or, if the Initiative has already commenced, when it commenced and the extent to which the processing activities relating to the Initiative are still ongoing)

Commenced January 2020

### Part B: Description of the processing

#### Nature of the processing

**Method(s) of collection** (e.g. online or paper-based forms completed by data subjects or feeds from other systems)

Paper based form – Hypertech Security “Consent to Disclosure of Personal Information” Form

|  |   |
|--|---|
| <b>Source(s) of the personal data being processed</b> (if personal data originates from third party sources, describe them)  | Direct from clients and or Clients nominated representative                       |
| <b>Matching or combination of datasets</b> (to what extent does the processing involve multiple datasets collected for separate purposes)  | Nil   |
| <b>Processing activities relating to the personal data</b> (how will personal data be processed after collection)  | Forwarded electronically to the relevant agency                                   |
| <b>Scope of data sharing with third parties</b> (you may want to refer to a data flow diagram or other materials explaining data flows)  | Limited to Name, Phone details, Email Address's, Photo ID images, CCTV Recordings |
| <b>Extent of automated decision-making</b> (describe extent to which decisions are made about data subjects without human intervention/review, e.g. through the use of automated algorithms) | Nil   |
| <b>Scope of the processing</b>   |   |
| <b>Categories of personal data</b> (identify each category of personal data processed, including any special category data and information relating to criminal convictions and offences)    | Name, Address, Phone Numbers, Email Address, Photo Image, CCTV Recordings         |

|   |   |
|---|---|
| <b>Categories of data subject</b> (e.g. staff, students, research participants, website visitors, device users, children, vulnerable adults)                          | Clients, client family members and or client's staff  |
| <b>Format of the personal data</b> (e.g. paper records, electronic documents, spreadsheets, databases, system records or other files)                                 | "Consent to Disclosure of Personal Information" Form – Manually filled in                   |
| <b>Storage location</b> (e.g. locked filing cabinets, document repositories, on-premise servers or storage devices, cloud-hosted services in UK, EU or international) | Held on our Secure server/NAS in our alarmed, access-controlled premises with CCTV coverage |
| <b>Duration and frequency of processing</b> (by reference to the relationship with the data subject or the nature of the Initiative)                                  | On demand by client   |
| <b>Volume of data subjects and records</b> (or an approximation where it is not possible to confirm precise numbers at present)                                       | 200 Approx.   |
| <b>Context of the processing</b>  |   |
| <b>Relationship with data subjects</b> (describe the proximity between Hypertech Security and the data subjects and how the relationship is established)              | Clients(residential/business) are our data subjects   |

|  |  |
|--|--|
| <b>Data subjects' expectations</b> (describe the extent to which the data subjects are aware of and expect their personal data to be used in connection with the proposed processing activities)                           | Clients (data subjects) are made aware of how their personal data is to be used by our "Consent to the disclosure of personal information" form  |
| <b>Use of new technology or novel approach</b> (describe the extent to which the processing activities involve the use of any technology or other approaches that may be considered state of the art, novel or unexpected) | N/A  |
| <b>Relevant matters of public concern</b> (describe any matters of public concern relating to the scope of the processing or the use of any particular technology or approach, if applicable)                              | N/A  |
| <b>Purposes of the processing</b>  |  |
| <b>Benefits to the data subject</b> (describe how the processing benefits the data subjects/individuals either directly or indirectly)   | The processing of the client's personal information to our agencies allows for a seamless process in these agencies being able to contact our clients in the case of an alarm incident quickly and with correct contacts etc |
| <b>Benefits to the organisation</b> (describe how the processing benefits the organisation either directly or indirectly)  | Efficiency and reduced risk, Customer satisfaction   |

|  |   |
|--|---|
| <b>Benefits to third parties</b> (describe how the processing benefits any third parties either directly or indirectly)  | Efficiency and reduced risk   |
| <b>Part C: Consultation process</b>  |   |
| <b>Input of internal stakeholders, experts and other professionals</b> (advice from parties including senior staff, specialists, IT experts, lawyers, security consultants, ethics advisers etc, where applicable)                                   | ASIAL<br>Office of the Australian Information Commissioner                                |
| <b>Advice from Data Protection Officer</b> (where applicable, obtaining the advice of the DPO is a mandatory requirement – this may be set out in a separate appendix/document)  | Mark Gordon – Hypertech Security – Personal Information & Information Security Manager    |
| <b>Input from data subjects (or their representatives)</b> (where relevant describe the views sought, consultation methodology or justification for not seeking input)   | Existing Client (data subjects) feedback input sought for formulation of our consent form |
| <b>Part D: Assessment of necessity and proportionality</b>   |   |
| <b>Lawful basis for processing</b> (identify the most appropriate ground(s) for lawful processing, explaining the rationale - see Appendix 3 for permissible grounds. For legitimate interests a separate legitimate interest assessment is needed.) | Office of the Australian Information Commissioner – Australian Privacy Principles         |

|   |  |
|---|--|
| <b>Fairness and transparency</b> (describe the means by which data subjects will be informed about the intended processing, e.g. fair processing notices, technical notifications, consent forms, participant information sheets) | Hypertech Security – “Consent to the Disclosure of Personal Information” form  |
| <b>Data minimisation</b> (describe the steps that will be taken to ensure that the amount of personal data is minimised and limited to what is strictly necessary both initially and on an ongoing basis)                         | Hypertech Security – “Consent to the Disclosure of Personal Information” form – Consent Authorisation – Client to approve which relevant record they consent to  |
| <b>Necessity of processing</b> (explain the extent to which the processing is necessary in relation to the purposes of the initiative)  | Required to allow communication from our agencies on receipt of alarm activations from our clients etc   |
| <b>Accuracy</b> (describe the steps taken to ensure data quality in terms of accuracy and freedom from bias, both initially and on an ongoing basis, e.g. verification techniques and how individuals can update their data)      | Consent form filled in directly by Client or Client nominated representative so minimal inaccuracy<br><br>Contact Details for Hypertech Security published on our consent form, privacy policy and via our website |
| <b>Storage limitation</b> (describe the steps taken to ensure that personal data are not retained longer than necessary in connection with the intended purposes of the processing)   | Only held as long per statutory or legal requirements  |

|  |   |  |  |   |
|--|---|--|--|---|
| <b>Security, integrity and confidentiality</b> (describe the steps taken to ensure the security of the personal data, including protection against personal data breaches)   | Held on our Secure server/NAS in our alarmed, access-controlled premises with CCTV coverage<br><br>Staff/Contractor – Confidentiality Agreements  |  |  |   |
| <b>Data subject rights</b> (describe the steps taken to ensure that data subjects are able to exercise their rights fully and effectively. Individuals have the right to be informed, and rights of access, rectification, erasure, objection and to stop automated decision making) | As per our Privacy Policy – Security & Protection   |  |  |   |
| <b>Third party processors</b> (where relevant, describe the steps taken to ensure the reliability of third parties processing the data on Hypertech Security’s behalf, and their compliance with data protection law)  | Contractor – Confidentiality Agreements<br>Statutory and legal requirements under Australian Law  |  |  |   |
| <b>International transfers</b> (identify any international transfers of personal data, whether or not to a third party processor, and the safeguards implemented in relation to such transfers)  | Not usually required<br>Only if authorised under Australian law or Court order<br>Only for an enforcement related activity (criminal matter)<br>If it was would deidentify the Personal Information |  |  |   |
| <b>Part E: Identification and assessment of risks (see Appendix 1 and Appendix 2 for example risks and assessment process)</b>   |   |  |  |   |
| <b>Ref No</b>  | <b>Source of risk and potential impact on data subjects</b> (including associated compliance and organisations risks)   | <b>Likelihood of harm</b> (see Appendix 2) | <b>Impact of harm</b> (see Appendix 2) | <b>Overall risk</b> (low, medium, high) |

|    |  |   |   |        |
|----|--|---|---|--------|
| 1. | Data is published which allows identification of an individual | 2 | 3 | Medium |
| 2. |  |   |   |        |
| 3. |  |   |   |        |
| 4. |  |   |   |        |
| 5. |  |   |   |        |

**Part F: Identification of controls and measures to eliminate or mitigate risk (of medium or high risks items in Part E)**

| <b>Ref No</b> | <b>Controls or measures to eliminate or mitigate risk</b> (changes to design or additional safeguards and measures) | <b>Effect on risk</b> (extent to which risk is eliminated or mitigated by the controls or measures) | <b>Residual risk</b> (any risk remaining after controls or measures have been implemented) |
|---------------|---|---|--|
| 1.            | Deidentify data where possible  | minimised   | Low  |
| 2.            | Destroy any personal information that is no longer required   | minimised   | Low  |
| 3.            | Apply password controls to Hypertech Security PC's  | minimised   | Low  |
| 4.            |   |   |  |
| 5.            |   |   |  |

| Part G: Implementation and integration of controls and measures  |               |  |                        |                                     |
|--|---------------|--|------------------------|-------------------------------------|
| Action   | Approved by   | Person(s) responsible  | Target completion date | Completed                           |
| Deidentify personal data where possible  | Mark Gordon   | Gordon Hutchison   | ASAP                   | <input checked="" type="checkbox"/> |
| Destroy any personal information that is no longer needed  | Mark Gordon   | Gordon Hutchison   | ASAP                   | <input checked="" type="checkbox"/> |
| Apply password controls to Hypertech Security PC's   | Mark Gordon   | Gordon Hutchison   | ASAP                   | <input checked="" type="checkbox"/> |
|  |               |  |                        | <input type="checkbox"/>            |
|  |               |  |                        | <input type="checkbox"/>            |
| Part H: Outcomes and sign-off  |               |  |                        |                                     |
| Residual risks that cannot be eliminated or mitigated (if any)   | Human error   |  |                        |                                     |
| Consideration of Data Protection Officer's advice (confirm whether advice accepted and implemented or rejected, and if rejected the reasons why) | Accepted      |  |                        |                                     |
| Sign-off   | Name and role | Mark Gordon – Privacy Information & Information Security Manager |                        |                                     |
|  | Date          | January 2020   |                        |                                     |

|  |              |
|--|--------------|
| <b>Frequency of review (usually at least annually)</b> | Annually     |
| <b>Next review date</b>                                | January 2021 |

## **Appendix 1 – Example types of risk associated with the processing**

### Risks to data subjects

- 
- Risk of processing being unlawful and/or regarded as unfair due to more personal data being collected than is necessary for the intended purposes of the processing
- Risk of personal data being inaccurate due to collection or processing methods or the nature of the personal data being processed
- Risk of personal data being retained longer than necessary or not properly managed so that duplicate records are created
- Risk of personal data being inadvertently manipulated due to human error or otherwise
- Risk of personal data being disclosed or accessed inappropriately due to inadequate access and disclosure controls
- Collection of personal data may be regarded as unnecessary and/or overly intrusive having regard to the objectives of the Initiative
- Risk of processing being unlawful and/or regarded as unfair due to scope and purposes of processing being extended inadvertently
- Use of new technologies, approaches or methods may constitute an unjustified intrusion on the data subjects' right to privacy
- Risk of processing being regarded as unfair due to complexity of processing activities/involvement of algorithmic analysis
- Risk of processing being regarded as unfair due to the combination of matching of multiple datasets
- Identifiers may be collected and linked which prevent data subjects from accessing or using a service anonymously
- Collection of personal data and linking identifiers may result in anonymisation being compromised
- Vulnerable data subjects may be particularly concerned about risks of identification or disclosure of personal data
- Processing of personal data may produce legal effects or similarly significantly affect the rights and interests of the data subject
- Processing of personal data may result in inappropriate inferences being made or discrimination being suffered by the data subject
- Disclosure of personal data may result in discrimination, victimisation and/or harassment

### Compliance risks

- Non-compliance with data protection laws, including the GDPR, Data Protection Act 2018, Privacy and Electronic Communications Regulations and other secondary legislation
- Non-compliance with common law duty of confidentiality
- Non-compliance with the Equality Act 2010 and other equality and human rights legislation
- Non-compliance with sector-specific legislation or standards

#### Associated organisational risks

- Risk of regulatory sanctions and fines
- Risk of reputational damage
- Risk of considerable financial expenditure to mitigate any risk that has materialised
- Risk of erosion of trust and confidence in processing activities resulting in loss of business
- Risk of investment returns being reduced or eliminated
- Risk of inaccurate, incomplete or outdated personal data having reduced value
- Risk of research or statistical objectives being compromised, skewed or false
- Risk of claims from individuals for compensation

## Appendix 2 – Risk assessment methodology

### Evaluation of likelihood of harm

| Likelihood score | 1                          | 2                                       | 3                                  | 4   | 5  |
|------------------|----------------------------|---|------------------------------------|---|--|
| Description      | Rare                       | Unlikely                                | Possible                           | Likely  | Almost certain   |
| Frequency        | Will probably never happen | Not anticipated to happen, but possible | Might happen or recur occasionally | Will probably happen or recur, but not persistently | Almost certain to happen or recur, possibly frequently |

### Evaluation of impact of harm

| Likelihood score | 1                           | 2                  | 3                        | 4   | 5                        |
|------------------|-----------------------------|--------------------|--------------------------|---|--------------------------|
| Description      | Very Low                    | Low                | Medium                   | High  | Very High                |
| Impact           | Unlikely to have any impact | May have an impact | Likely to have an impact | Highly probably it will have a significant impact | Will have a major impact |

Overall evaluation of risk

|        |               |            |              |              |            |                    |
|--------|---------------|------------|--------------|--------------|------------|--------------------|
| Impact | Very High (5) |            |              |              |            |                    |
|        | High (4)      |            |              |              |            |                    |
|        | Medium (3)    |            |              |              |            |                    |
|        | Low (2)       |            |              |              |            |                    |
|        | Very Low (1)  |            |              |              |            |                    |
|        |               | Rare (1)   | Unlikely (2) | Possible (3) | Likely (4) | Almost certain (5) |
|        |               | Likelihood |              |              |            |                    |

## **Appendix 3 – Lawful basis for processing personal data**

### **Personal data**

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

- (a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
- (b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- (c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- (d) Vital interests: the processing is necessary to protect someone's life.
- (e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. Hypertech Security's public tasks revolve around Electronic Security. All research can come under this lawful basis.
- (f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. This cannot apply if Hypertech Security is processing data to perform its public tasks. A legitimate interests assessment may be required.

### **Special category data**

If you are processing special category data (information about an individual's race, ethnic origin, political opinion, physical or mental health, religion, trade union membership, genetics, biometrics, sexuality or sex life) then you also need a further lawful basis set out in Article 9 of GDPR. At least one must apply whenever you process special category data. The main Article 9 lawful bases are outlined here, though others also exist. Please seek further advice from the Data Protection Officer if required:

- (a) Explicit consent: the individual has given their explicit consent to the processing of their personal data for the specific purpose.

- (b) Employment law: the processing is necessary for pursuing obligations set out in employment law.
- (c) Vital interests: the processing is necessary to protect someone's life where they are incapable of giving consent.
- (d) Substantial public interest: the processing is necessary for reasons in the substantial public interest where it will safeguard the rights and interests of the individual.
- (e) Medical purposes: the processing is necessary for the purposes of preventive or occupational medicine, or the provision of health care.
- (c) Research purposes: the processing is necessary for purposes of scientific or historical research in the public interest. This lawful basis will apply to all research conducted by Hypertech Security involving special category data.

## HYPERTECH SECURITY - PASSWORD POLICY

Employees & Contractors at Hypertech Security must access a variety of IT resources, including computers and other hardware devices, data storage systems, and other accounts. Passwords are a key part of Hypertech Security's strategy to make sure only authorised people can access those resources and data.

All employees who have access to any of those resources are responsible for choosing strong passwords and protecting their log-in information from unauthorised people.

The purpose of this policy is to make sure all Hypertech Security's resources and data receive adequate password protection. The policy covers all employees who are responsible for one or more account or have access to any resource that requires a password.

### Password creation

- All passwords should be reasonably complex and difficult for unauthorised people to guess. Employees should choose passwords that are at least eight characters long and contain a combination of upper- and lower-case letters, numbers, and punctuation marks and other special characters. These requirements will be enforced with software when possible.
- In addition to meeting those requirements, employees should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like "password," "password1" and "Pa\$\$w0rd" are equally bad from a security perspective.
- A password should be unique, with meaning only to the employee who chooses it. That means dictionary words, common phrases and even names should be avoided. One recommended method to choosing a strong password that is still easy to remember: Pick a phrase, take its initials and replace some of those letters with numbers and other characters and mix up the capitalization. For example, the phrase "This may be one way to remember" can become "TmBOWTr!".
- Employees must choose unique passwords for all of their company accounts and may not use a password that they are already using for a personal account.
- All passwords must be changed regularly, with the frequency varying based on the sensitivity of the account in question. This requirement will be enforced using software when possible.
- If the security of a password is in doubt— for example, if it appears that an unauthorised person has logged in to the account — the password must be changed immediately.
- Default passwords — such as those created for new employees when they start or those that protect new systems when they're initially set up — must be changed as quickly as possible.

### Protecting passwords

Employees/Contractors may never share their passwords with anyone else in the company, including co-workers, managers, administrative assistants, IT staff members, etc. Everyone who needs access to a system will be given their own unique password.

- Employees may never share their passwords with any outside parties, including those claiming to be representatives of a business partner with a legitimate need to access a system.
- Employees must refrain from writing passwords down and keeping them at their workstations. See above for advice on creating memorable but secure passwords.





## Consent to the Disclosure of Personal Information\*

This form must be provided to Hypertech Security by the person granting consent.

### 1. Personal details

|              |  |
|--------------|--|
| Family name  |  |
| First name   |  |
| Address      |  |
| Home phone   |  |
| Mobile phone |  |
| Email        |  |

### 2. Consent Authorisation

I hereby consent to the following records and/or personal details/information: (tick relevant boxes)

- ☐ Name
- ☐ Address
- ☐ Home Phone
- ☐ Mobile Phone
- ☐ Email
- ☐ Photo
- ☐ Other (Please specify) .....

Being disclosed by Hypertech Security to: (tick relevant boxes)

- ☐ Central Monitoring (back to base services)
- ☐ Monitoring Excellence (back to base services)
- ☐ Guard Patrol (alarm response/patrol)
- ☐ Strata Plan Management services
- ☐ Other (Please specify) .....



### 3. Consent declaration

(tick relevant boxes)

- ☐ I give consent to Hypertech Security to collect and use my personal and sensitive information as disclosed in this Disclosure of Personal Information Form.
- ☐ I have read and understand the Disclosure of Personal Information Form.
- ☐ I have been given the opportunity to clarify any information in the Disclosure of Personal Information Form.

Full name of client or nominated representative signing this declaration:

If applicable name of client who you are representing and signing on behalf of:

Signature:

Date:

- \* Does not include Personal Information that is required to be disclosed under Australian law or a court/tribunal order by Hypertech Security. "Personal Information" means information or an opinion (including information forming part of a database), whether true or not, and whether recorded in a material form or not, about a natural person whose identity is apparent, or can be ascertained, from the information or opinion.

### Contact Details:

**Privacy Information & Information Security Manager**  
**Hypertech Security**  
**PO Box 382**  
**Winston Hills NSW 2153**  
**Australia**  
**P: 02 9631 1008**  
**E: [info@hypertech.com.au](mailto:info@hypertech.com.au)**



## **Confidentiality Agreement – Between Hypertech Security and XXXX**

This confidentiality agreement is effective as of:

This confidentiality agreement is made by:

Hypertech Protection Services Pty Ltd (T/A Hypertech Security) ABN: 16 084 642 866  
and is between Hypertech Security and XXXX

Business Name & ABN (If Applicable): XXXX

Name: #####

Address:

The two participants shall from hereon be referred to collectively as 'the parties' for the remainder of this agreement.

For due and thorough consideration, the sufficiency and receipt of which are hereby acknowledged,  
the parties agree to the following terms:

**1. Purpose** – Hypertech Security and Xxxx shall enter into a relationship in which certain sensitive and privileged information may be shared with Xxxx

**2. Definition** – For the purpose of this agreement, sensitive, privileged, or confidential information may include but is not limited to:

- Client staff names
- Client personal address
- Client date of birth
- Client gender
- Client email address
- Client contact phone numbers
- Client CCTV recorded images
- Client photographs
- Clients employment details



- Client license details
- Client trade confidential/sensitive information
- Hypertech Security trade confidential/sensitive information

and any other information obtained by Xxxx as a result of the relationship entered in to through this agreement which may be relevant to or have implications for the lawful and reasonable operations of Hypertech Security

### **3. Non-disclosure of privileged information**

Upon signing this agreement Xxxx agrees not to use any sensitive, privileged, or confidential information disclosed to them by Hypertech Security for any purpose other than the intended use as would be relevant to the relationship entered into by the parties.

Xxxx for any purpose other than the intended use as would be relevant to the relationship entered into by the parties.

Xxxx shall not disclose the relevant confidential information to any other party without express permission from Hypertech Security.

Xxxx agrees to take all possible measures to protect the security and secrecy of any sensitive, privileged, or confidential information they may be exposed to during and secrecy of any sensitive, privileged, or confidential information they may be exposed to during and after their involvement with Hypertech Security.

### **4. Ownership of information**

All privileged information as defined in this agreement shall remain the exclusive property of Hypertech Security and its relevant clients, and Xxxx agrees that they have no right to use this information in any way except as directed by Hypertech Security.

### **5. Notice/termination**

This agreement may only be terminated by express agreement between Hypertech Security and Xxxx

### **6. Remedies**

In the event that Xxxx breaches this agreement, Hypertech Security reserves the right to commence court proceedings against Xxxx in order to obtain compensation for this breach unless a satisfactory remedy can be settled on outside of court.

Final agreement

Date: \_\_\_\_\_

Hypertech Security

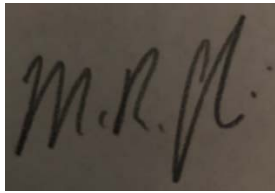
PO Box 382

Winston Hills

NSW, 2153

Hypertech Director Name: Mark Gordon

Signature:

A rectangular image showing a handwritten signature in dark ink on a light-colored background. The signature appears to be 'M.R. Gordon' written in a cursive, stylized font.

Xxxx

#### - Signature: \_\_\_\_\_

**KEEP A COPY OF THIS AGREEMENT FOR YOUR RECORDS**