

Guide to Goods & Services

Note: The items identified in green (left column) are standard items included in your Annual SaaS Subscription

Additional Services in blue and Pricing is listed in Schedule 2

Reference Numbers relate to explanation of service in Additional Goods & Services from page 2 of Schedule 3

IDS Reception/Aviation VMS Standard Goods & Services	Additional Goods & Services
1. IDS Reception VMS Setup <ul style="list-style-type: none"> <input type="checkbox"/> 1.1 Account Configuration <input type="checkbox"/> 1.2 Tenant Branding <input type="checkbox"/> 1.3 IDS Reception VMS User Accounts <input type="checkbox"/> 1.4 Historical Data Import <input type="checkbox"/> 1.5 Unique Tenant Domain 	<ul style="list-style-type: none"> <input type="checkbox"/> 1.6a Account Configuration additional hours <input type="checkbox"/> 1.7a Historical Data Import additional hours <input type="checkbox"/> 1.8a Data Entry <input type="checkbox"/> 1.9a Additional Sub tenant Setup <input type="checkbox"/> 1.9.1 Onsite Hardware configuration, installation and testing
2. Training <ul style="list-style-type: none"> <input type="checkbox"/> 2.1 Training Materials <input type="checkbox"/> 2.2 Phone/Skype Training 	<ul style="list-style-type: none"> <input type="checkbox"/> 2.4a On Site Training <input type="checkbox"/> 2.5a Customised Training Materials
3. Hosting and Security <ul style="list-style-type: none"> <input type="checkbox"/> 3.1.0 Physical Security <input type="checkbox"/> 3.1.1 Application Security <input type="checkbox"/> 3.1.2 Data Security <input type="checkbox"/> 3.1.3 Reliability <input type="checkbox"/> 3.1.4 Disaster Recovery <input type="checkbox"/> 3.1.6 Performance <input type="checkbox"/> 3.1.7 Monitoring <input type="checkbox"/> 3.1.8 Compatibility <input type="checkbox"/> 3.1.9 Data Breach Procedure Response Plan 	<ul style="list-style-type: none"> <input type="checkbox"/> 3.2a Tenant Dedicated Server & Set Up <input type="checkbox"/> 3.3a Data Optimisation <input type="checkbox"/> 3.4a SMS Gateway Configuration
4. Online Ticket Support Process <ul style="list-style-type: none"> <input type="checkbox"/> 4.1 Ticket Support - support@idsecurity.com.au <input type="checkbox"/> 4.2 Approvals Process 	
5. Telephone Support <ul style="list-style-type: none"> <input type="checkbox"/> 5.1 User Telephone Support <input type="checkbox"/> 5.2 Visitor Telephone Support <input type="checkbox"/> 5.3 Technical Support 	<ul style="list-style-type: none"> <input type="checkbox"/> 5.4a Onsite Technical Services
6. Software Updates <ul style="list-style-type: none"> <input type="checkbox"/> 6.1 Included Customisations 	<ul style="list-style-type: none"> <input type="checkbox"/> 6.2a New Modules & Plugins <input type="checkbox"/> 6.3a Additional Customisations
7. IDS Reception VMS Notifications	
8. Supported Hardware <ul style="list-style-type: none"> <input type="checkbox"/> 8.1 Order and Supply of Hardware 	
9. Kiosk Maintenance & Support	<ul style="list-style-type: none"> <input type="checkbox"/> 9.1a Onsite Technical Support <input type="checkbox"/> 9.2a Onsite Technical Services After Hours
10. Additional IDS Reception VMS Modules	<ul style="list-style-type: none"> <input type="checkbox"/> 10.1a Purchase of Additional Modules <input type="checkbox"/> 10.2a Integration of Hardware (API's) <input type="checkbox"/> 10.3a Access Control Integration

Description of Goods, Services and applicable Service Level

Note: The items identified in red are standard items identified in blue are additional items

Name of Good or Service	Description of Goods, Services and applicable Service Level
1. IDS Reception VMS Setup	Prior to your commencement date, Identity Security will provide the Administrator IDS Reception VMS Setup Guide with instructions for the Issuing Tenant Administrator can configure their preferences.
1.1 Account Configuration	<p>Identity Security will create an Administrator Login for the Tenant and one Subtenant Administrator Login for each Subtenant as well as the required workstation outline in the particulars.</p> <p>Your will be issued with their own unique pre registration Kiosk link which can be hyper-linked to their website, for example https://vmspr.identitysecurity.com.au/xxxx</p>
1.2 Tenant Branding	Identity Security will upload your logo in Module 1 & 2 and customise the display to match your Tenant branding.
1.3 IDS Reception VMS User Accounts	The Issuing Body and Subtenant Administrators are responsible for the setup of these logins entering correct data and deactivating operators who have left the company.
1.4 Historical Data Import	Identity Security will import and test 12 months of formatted and cleansed data inclusive of the set up fee. A maximum of 3 hours data cleansing or reformatting. If the data has not been cleansed you may be charged additional hours see 1.8a Data Cleansing additional hours
1.5 Unique Tenant Domain	IDS Reception VMS can be configured to a unique Tenant domain to accommodate unique customisations for your Tenant.
<input type="checkbox"/> 1.6a Account Configuration additional hours	Identity Security will configure user accounts on behalf of a Tenant. This could include contacting the account holder, creating user accounts on the Tenants behalf. Cost of service will be quoted upfront.
<input type="checkbox"/> 1.7a Additional Subtenant Setup	<p>In the event a new Sub tenant would like to issue VIC's after the commencement date the Tenant must provide confirmation in writing for IDS to configure a new account to support@idsecurity.com.au</p> <p>Setup fee includes the configuration of the account, online training, access to manuals</p>
<input type="checkbox"/> 1.8a Data Cleansing additional hours	Identity Security will assess provided data prior to import. If data requires more than 3 hours of reformatting we will inform you and provide a quotation or instruction to complete the data cleansing process (3c)

<p>❑ 1.9a Data Entry</p>	<p>Identity Security can enter backed data from manual forms. Please email scanned forms to support@idsecurity.com.au How's will be estimated upfront prior to commencement of work.</p>
<p>❑ 1.9.1a Onsite Hardware Testing and Configuration</p>	<p>Identity Security offers of technicians to carry out onsite hardware testing configuration to selected clients. This can include;</p> <ul style="list-style-type: none"> ● Kiosk Set Up & Technical Configuration (3g) ● OCR module and testing of Web Services (3h) ● Installation and testing of printers (8f) <p>Pricing is subject to variation if access to the environment is not available at the time arranged or infrastructure is not prepared for work to be carried out.</p>
<p>2. Training</p>	<p>A training date will be set on an agreed date on or after the commencement date.</p> <p>Online training is included in the subscription fee for all Tenant operators and approved Subtenants on or after the commencement date. 2.3 Phone or Skype Training.</p> <p>Onsite training is subject to travel costs which will be quoted upfront. 2.4a On Site Training</p>
<p>2.1 Training Materials</p>	<p>IDS Reception VMS training materials consist of the following;</p> <ol style="list-style-type: none"> 1.Subtenant and Tenant Operator Cheat Sheet 2. Administrator and Subtenant Administrator Cheat Sheet 3. Access to Online Help Menu <p>These documents generic and are in word format and be edited by the Tenant to suit your internal procedures.</p> <p>These documents are also downloadable from the Contact Support Menu/Help Documents in IDS Reception VMS.</p>
<p>2.2 Phone/Skype Training</p>	<p>One hour of online training via Skype or any other technology which should be configured at least 2 hours prior to the arranged training time to allow for troubleshooting if required.</p> <p>This can either be train the trainer or with a group session which will be a screen sharing session which Identity Security will initiate.</p> <p>Cheat Sheets and Manuals will be emailed a day prior to the meeting organiser for printing.</p>

	Attendees may bring their laptop into the training.
<p>❑ 2.4a On Site Training</p>	<p>Onsite training is available for a full day or half day session. Two sessions can be conducted in a half day. Travel expenses are in addition to the subscription fee.</p> <p>All training materials will be provided at the training session. The Tenant may be asked to reproduce training materials if numbers exceed 20 attendees.</p> <p>Tenant should manage the training room and invitations to the training at least one week prior to the training and confirm attendance.</p>
<p>❑ 2.5a Customised Training Materials</p>	<p>Training Materials can be customised with Tenant Branding and edited to suit customer requirements.</p>
<p>3. Hosting and Security</p>	<p>IDS Reception VMS Software as a Service is managed on an external server by Amazon Web Services in Sydney NSW in Australia in accordance with Australian Data Security. AWS Service Level Agreement https://aws.amazon.com/ec2/sla/</p>
<p>3.1 Physical Security</p>	<p>Identity Security employees use the following methodologies for physical. Identity Security reserves the right to update these procedures at any time in order to improve our service with Customisers prior written consent.</p> <ul style="list-style-type: none"> > The data centre where the VMS is hosted is ISO27001 certified > Access to the infrastructure that is used to host IDS Reception VMS is restricted by multiple layers of physical security.
<p>3.1.0 Application Security</p>	<p>Identity Security use the following methodologies for application security. Identity reserves the right to update these procedures at any time in order to improve our service.</p> <ul style="list-style-type: none"> > The approved Asymmetric/public key algorithm is Rivest-Shamir_Adleman(RSA) with 2048 bit key length. > The approved symmetric encryption algorithm is Advanced Encryption Standard (AES) with minimum 256 bit key length (AES-256) > The approved hashing algorithm is Secure Hashing Algorithm 2 (SHA-2) a minimum of 256 bit key length (SHA-256) > All applications encrypt data in transit using Transport Layer Security (SSL) v1.2 using the approved algorithms. > All certification, private keys and passwords are stored securely in a key management system > The VMS is compliant with the mitigation as defined in the Open Web Application Security (OWASP)


	<ul style="list-style-type: none"> ➤ All components of the system are updated to address security vulnerabilities and feature enhancements. The system should not be exposed to any vulnerability that is Critical or High by NIST (https://nvd.nist.gov/home.cfm, under the Common Vulnerability Scoring System, for more than 30 days ➤ The application is tested regularly for vulnerabilities and prior to rollouts of all software updates
3.1.2 Data Security	<p>Identity Security use the following methodologies for security of your data. Identity reserves the right to update these procedures at any time to improve our service.</p> <ul style="list-style-type: none"> ➤ Where the data is stored in a database, the database is encrypted using Transparent Database Encryption (TDE) using Advanced Encryption Standard (AES) with a minimum of 128 bit key length (AES-128) ➤ Using TDE with AES automatically implements Cipher Block Chaining (CBC) and random Initialization Vectors (IV or "salt") ➤ When implementing TDE, the Database Encryption Key (DEK) must be encrypted using a Server Certificate which has been created using the DER file format and have the CER extension. The certificate must have a minimum key length of 2048 ➤ Cryptographic keys must be stored securely and managed throughout their lifecycle. Access to them should be restricted, audited and logs retained. ➤ IDS holds the root access of the database and hence can view the data unencrypted.
3.1.3 Reliability	<p>Identity Security use the following methodologies for reliability. Identity reserves the right to update these procedures at any time to improve our service.</p> <ul style="list-style-type: none"> ➤ IDS Reception VMS is available 24/7 365 days per year ➤ The hosting environment is fault tolerant and highly available ➤ IDS Reception VMS meets uptime reliability of 99.9%, which equals a total outage time of 8.75 total hours in any 365 day period. ➤ IDS Reception VMS uses validation techniques and business rules to minimise duplication of data and erroneous input ➤ IDS takes all steps necessary to avoid data corruption including log backups and use RAID storage, UPS and circuit protection systems
3.1.4 Disaster Recovery	<p>Identity Security users the following methodologies for data recovery.. Identity reserves the right to update the these procedures at any time to improve our service.</p> <ul style="list-style-type: none"> ➤ IDS Reception VMS is geographically dispersed

	<p>between two locations so if one is unavailable the system will operate from another location.</p> <ul style="list-style-type: none"> ➤ The restore of the system back to normal is a maximum of four hours. ➤ A message of outage, including planned maintenance will be displayed to users
3.1.6 Performance	<ul style="list-style-type: none"> ➤ IDS Reception VMS aims to provide a quick response to user actions, typically less than 5 seconds. ➤ If an IDS Reception VMS user is experiencing slower speeds than this, which are not related to issues with internet connectivity consistently user should contact IDS for further troubleshooting of the issue ➤ Performance issues relating to data storage may result in data optimisation services which may take ➤ Tenants on dedicated server may be charged a service fee for data optimisation.
3.1.7 Monitoring	<ul style="list-style-type: none"> ➤ IDS Reception VMS is monitored 24 x7 for common web-based attacks and any incident will be reported to the Tenant ➤ Application logs are analyzed for suspicious behaviour and suspicious behaviour and any incidents will be reported ➤ Application logs are retained for 18 months and accessible from Issuing Body Login in IDS Reception VMS > IDS Reception VMS ➤ Reports > Audit Trail ➤ IDS Reception VMS does not allow users to upload any malicious software
3.1.8 Compatibility	<ul style="list-style-type: none"> ➤ IDS Reception VMS is compatible with Internet Explorer, Firefox, Chrome and Safari Browsers. Where possible the Tenant should have the ➤ Web Pre Registration is built in a responsive design which
3.1.9 Data Breach Procedure Response Plan	<p>In the event of a data breach (or suspected breach) Identity Security is prepared to act quickly and determine whether it is likely to result in serious harm and whether it constitutes an NDB (Notifiable Data Breach)</p> <p>Process where a breach occurs or is suspected</p> <p>Alert</p> <p>Where a privacy breach is known or have occurred(or is suspected) any member of Identity Security staff must, within 24 hours, alter a Member of the Executive in the first instance.</p> <p>They will provide the following information(if known)</p>

	<ol style="list-style-type: none"> a) When the breach occurred (date and time) b) Description of the Breach(type of personal information involved) c) Cause of breach (if known) otherwise how it was discovered d) Which systems(s) if any were affected? e) Which directive/faculty/institute is involved? f) Whether correct action has occurred to remedy or ameliorate the breach (or suspected breach) <p>Severity Assessment Member of Executive will assess potential impact using the following criteria</p> <ol style="list-style-type: none"> a) Is personal information involved b) Is the personal information of a sensitive nature c) Has there been unauthorised access to personal information, or unauthorised disclosure of person information, or loss of personal information in circumstances where access to information is likely to occur? <p>Determining Severity</p> <ol style="list-style-type: none"> a) The type and extent of personal information involved b) Whether multiple individuals have been affected c) Whether the information is protected by any security measure(password protection or encryption) d) The person or people who now have access e) Whether there (or could be) a real risk of serious to the affected individuals f) Whether there could be media or stakeholder attention as a result of the breach or suspected breach <p>Within 24 hours of being altered Member of Executive must notify Privacy Officer</p> <p>Privacy Officer to issue pre-emptive instructions On receipt of the communication by the relevant member of the Executive, the Privacy Officer will take preliminary view as to whether the breach(or suspect breach) may constitute an NDB.</p> <p>Management of Data Breach The Response Team method of responding to a data breach and each incident must be dealt with on a case by basis by assessing the circumstances and associated risks to inform the appropriate course of action.</p> <p>The following action must be undertaken by the Response Team as appropriate</p> <ul style="list-style-type: none"> • Immediately contain the breach (if this has not already occurred) Corrective action may include;retrieval of recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system. • Evaluate the risks associated with the breach including collecting and documenting all available
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>evidence of the breach having regard for the type of information</p> <ul style="list-style-type: none"> • Call upon the expertise of, or consult with, relevant staff in the particular circumstances • Engage a third party if necessary • Make recommendation to Privacy Officer as to whether the breach constitutes an NDB for the purpose of mandatory reporting to the OAIC and the practicality of notifying affected individuals • Consider a media communication strategy <p>The Response Teams must undertake its assessment within 48 hours of being convened.</p> <p>Notification Having regard to the Response teams recommendation and whether there are reasonable grounds to suspect that an NDB has occurred, the Privacy Officer must prepare a prescribed statement and provide a copy to the OAIC as soon as practicable (and no later than 30 days after becoming aware of the suspected breach)</p> <p>If practicable, Identity Security must also notify each individual to whom the relevant personal information relates. Where impracticable, Identity Security must take reasonable steps to publicise statement (including on the website)</p> <p>Contact Director of Human Resources admin@idsecurity.com.au 03 9645 3450</p>
<p>❑ 3.2a Tenant Dedicated Server (3e)</p>	<p>Configuration of IDS Reception VMS on your Tenant only dedicated server. It includes the configuration following;</p> <ul style="list-style-type: none"> > Firewalls > Secure Certificates > Application Layered Security > Mail Server Configuration > Data Backup > Disaster recovery fall back site > Branding and Configuration of agreement, and Master Account
<p>❑ 3.3a Data Optimisation</p>	<p>At the customer request Identity Security offers a Data Optimisation in aid of increasing the application performance. This service is quoted upfront any typically workload is 5 - 10 working days. <i>Applies only to Tenants on their own dedicated server.</i></p>
<p>❑ 3.4 SMS Gateway Configuration</p>	<p>For SMS notifications the customer can request SMS notifications;</p> <p>The Tenant should specify the types of notifications to be received for configuration purposes. ie. Notify ASIC Sponsor of VIC Holder arrival, Return expired VIC etc.</p>

	<p>Additional charges apply for the receipt of messages which is based on volume. The Tenant should provide a volume of the amount of messages. Identity will provide plan options whereby the Tenant should choose the agreed plan prior to configuration of the gateway and accept charges and payment terms.</p>
<p>4. Online Support</p>	<p>Online Ticket Support is available 24/7 to all IDS Reception VMS Operators via contact support or emailing support@idsecurity.com.au</p>
<p>4.1 Online Ticket Support Process</p>	<p>Online issues are responded to immediately with a Ticket Support number Initial Response time is up to 2 hours from 8am to 8pm EST</p> <p>The request will be categorised and prioritised and assigned to our customer support staff.</p> <p>Support Categories Task = Customisation, or, General Fix Problem = Blocker or Technical Issue Question = General Question and User Support</p> <p>Response Times during business hours 8am to 8pm Tasks as assigned a priority and issued a ticket given with a due date within 2 hours during business hours.</p> <p>Priority Levels: Low, Normal, High, Urgent Low : No set time frame. Will be monitored until complete Normal: Within 28 working days unless otherwise notified High: Within 2 working days unless otherwise notified Urgent: If not immediately within 2 hours resolution time unless otherwise notified</p>
<p>4.2 Approvals Process</p>	<p>When an acknowledgement is formerly required by IDS an approval request will be sent to the Project Manager or Authorised Person.</p> <p>This could be for one of the following reasons;</p> <ul style="list-style-type: none"> - Acknowledgement of client responsibilities - Purchase Request for additional customisations or variations of services or expenses to a project - Notification of Change Request to a project which may or may not have a cost impact to the project <p>By clicking 'Approve' the Project Manager or Authorised person is accepting this change.</p>

<p>5.Telephone Support</p>	<p>Telephone Answering Service is available 24 hours a day, 7 days a week and may be utilised by calling the IDS call centre on 1300 70 90 28.</p> <p>Support Response Times Response times apply during business hours 8am to 8pm EST.</p> <p>If the call is unanswered by our internal staff the user will receive a phone call back within 2 hours during business hours.</p> <p>If the issue is not resolved on the spot issue will be ticketed and resolved via our Online Ticket Support Process.</p>
<p>5.1 Telephone Customer Support IDS Reception Users</p>	<p>Customer support is available to the following user roles; Administrator, Tenant Operators, Subtenant Administrators and Subtenant Operators on the paid telephone support plans only. See Price list for plans with telephone support.</p>
<p>5.2 Telephone Customer Support IDS Visitors</p>	<p>All IDS Reception VMS Visitor Users issues should directed to the Tenant unless otherwise arranged.</p> <p>On occasion IDS may request to speak directly to a visitor for technical troubleshooting in order to improve the usability of the application.</p>
<p>5.3 Technical and Hardware Support</p>	<p>IDS will troubleshoot issues and assign to either our technical staff for resolution via the Online Ticket Support Process.</p> <p>Some issues may be a result of the Tenants IT configuration of which the issue will be referred to your IT department for further troubleshooting.</p> <p>All hardware purchased from IDS will be support via our Ticketing Process. In some cases we may refer you to our supplier for additional troubleshooting. Identity Security will ensure hardware is fully operational before closing the ticket. <i>See Price List for hardware supported and supplied by IDS.</i></p>
<p> 5.4a Onsite Technical Support</p>	<p>In certain instances, IDS may be required to attend onsite to resolve an issue. If this occurs, IDS will notify you and you may be required to pay additional fees. Any such fees will be quoted by IDS on a case-by-case basis.</p>
<p>6. Software Updates</p>	<p>IDS Reception VMS an ever evolving application which is constantly being client site tested and enhanced by their feedback.</p>

6.1 Included Customisations	Identity Security will include these customisations within the subscription fee.
<input type="checkbox"/> 6.2 New Modules & Plugins	<p>New Modules and plugins may be introduced from time to time of which Identity Security will forward correspondence of their availability and costings.</p> <p>Tenants can request these modules at anytime via contact with IDS and a purchase order.</p>
<input type="checkbox"/> 6.3a Additional Customisations	<p>Additional customisations outside the 6.1 Included Customisations and the listed Product Specifications may incur Customised Software Development Fee under IDS Agile Development Agreement.</p> <p>Customisations more than 40 hours of estimated development are subject to a quotation and scoping fee which is payable prior to scoping work and documentation is produced.</p> <p>The Tenant may decide to not have all or part of the works completed after documentation of which the Scoping Fee will still apply. (3j Module Configuration and Scoping Fee)</p> <p>A purchase order must be issued prior to both to the commencement of the scoping and then the customised development.</p> <p>The Tenant authorised person must sign off on the requirements, design and development prior to the development being costed.</p> <p>Identity Security have the right to decline the customisation if the requirement is conflicting with another function of the application.</p> <p>Identity Security may offer newly developed customisations to other Tenants should it be relevant to their requirements in the future.</p>
7. IDS Reception VMS Notifications	<p>Identity Security will send notifications of all updates to IDS Reception VMS. These notifications could relate to Product Updates or other important relevant information.</p> <p>All IDS Reception VMS Users can opt out via IDS Reception VMS login to not receive email notifications however they will still be sent to their notifications in box.</p>
8. Supported Hardware	<p>Identity Security offers customer and technical support to hardware listed in our price list which has been purchased from Identity Security.</p> <ul style="list-style-type: none"> • Zebra G Services Printer

	<ul style="list-style-type: none"> • Bleed-through labels and Backing Stickers • Standard Reception Yellow • Snapshell OCR Module • Diamond Kiosk <p>Identity Security cannot ensure compatibility with other hardware with IDS Reception VMS.</p> <p>A configuration fee may apply to unsupported hardware and will be quoted upfront accordingly.</p>
<input type="checkbox"/> 8.2a Ordering and Supply of Hardware	<p>Purchase of hardware and peripherals can be made via Identity Security's ID Store at idsecurity.com.au upfront with credit card or paypal.</p> <p>Alternatively payment can be made via Purchase order, invoice and EFT payment.</p> <p>Payment of hardware is required prior or on delivery unless an account has been previously arranged with Identity Security.</p> <p>Delivery is within 5 business days unless otherwise notified.</p>
9. Kiosk Maintenance & Support	<p>Kiosk maintenance and support is inclusive of the subscription fee.</p> <p>Technical Issues will be escalated via our Online Ticket Support Process.</p> <p>Issues in relation to kiosk unit, web-services and equipment supporting the kiosk solution maybe referred to our supplier for additional troubleshooting and support of which IDS will coordinate.</p> <p>3 hours of onsite support (during business hours) per annum per kiosk is included within the annual subscription fee. This does not include the initial installation, testing and setup of the kiosk.</p>
<input type="checkbox"/> 9.1a Kiosk Onsite Technical Services	<p>Additional hours of onsite support outside the included hours per kiosk at billable at the Onsite Technical Support Rate (7d)listed in our Price List.</p>
<input type="checkbox"/> 9.2 a Onsite After Hours Services	<p>Emergency work carried out outside of business hours on or off site may be subject to our Emergency after hours rate listed in our price list.</p>
10. Addition of Modules	<p>IDS Reception VMS Modules are now available. Each module feature inclusions are listed in the Product Specifications document.</p>
<input type="checkbox"/> 10.1a Purchase of Additional Modules	<p>A list of the additional available modules are listed in Section 4. Of the Price List.</p>

	<p>The Tenant may add or vary the module in accordance with the product specifications. Upto 30 hours of customisations are inclusive of the module fee excluding the ASIC Issuing and Management Module which is on a pay as you use basis (5e)</p> <p>An additional module attracts a Module Configuration and Scoping fee of which the core module will be customised to suit the Tenant requirements(3j)</p> <p>A purchase order should be produced before scoping proceeds.</p> <p>Identity Security will produce a design document and quotation inclusive of the scoping fee.</p> <p>Prior to development the Tenant Project Manager are required to sign off on the requirements before development commences.</p> <p>The Tenant should test and approve prior to GO LIVE and sign off with Identity Security by ticket support communications and in accordance with Tenant administrative policies.</p>
<p>❑ 10.2a Integration of New Hardware (API's)</p>	<p>Other hardware and systems may be integrated with IDS Reception which will attract Scoping Fee(3h)</p> <p>This work will be carried out via a IDS Agile Customised Development Agreement.</p>