

## CONTRACTOR PROCEDURES

- 5.7 Without limiting any other obligations of the Contractor under this Section, the Contractor must:
- a) establish, maintain, enforce and continuously improve safety and security procedures and safeguards against the unauthorised interference with, use, destruction, loss or alteration of Customer Data and the Customer's other Confidential Information; and
  - b) allow the Customer's annual audits to verify current safety and security procedures and safeguards continue to meet required standards.

## COMPLIANCE WITH SECURITY REQUIREMENTS

- 5.8 The Contractor must comply with the security requirements set out in Item 25 of the General Order Form, together with reasonable, whole of government, standard security requirements of the Customer from time to time communicated to the Contractor, including security requirements relating to access to, and use of, any data, information systems or facilities provided by the Customer (**Security Requirements**).
- 5.9 If the Contractor becomes aware that the security of any of the Customer's Data or Personal Information has been compromised, or that such Customer Data or Personal Information has been or is reasonably expected to be subject to a use or disclosure not authorized by this Agreement (an **Information Security Incident**), Contractor shall:
- (a) promptly (and in any event within 24 hours of becoming aware of such Information Security Incident), notify the Customer, in writing, of the occurrence of such Information Security Incident;
  - (b) investigate such Information Security Incident and conduct a reasonable analysis of the cause(s) of such Information Security Incident;
  - (c) provide periodic updates of any ongoing investigation to the Customer;
  - (d) develop and implement an appropriate plan to remediate the cause of such Information Security Incident to the extent such cause is within Contractor's control; and
  - (e) co-operate with the Customer's reasonable investigation or the Customer's efforts to comply with any notification or other regulatory requirements applicable to such Information Security Incident.

## CUSTOMER DATA

- 5.10 The Contractor must take all reasonable technical, administrative, and physical steps to ensure that:
- (a) any Customer Data held or controlled by the Contractor in connection with this Customer Contract, irrespective of where it is stored, is protected against misuse, loss, unauthorised access, interference, modification or disclosure; and
  - (b) the Customer Data is accessed only by authorised Contractor Personnel whose role requires access to the Customer Data in order for the Contractor to perform its obligations under this Customer Contract.
- 5.11 The Customer will notify the Contractor of respective data sensitivity in line with the NSW Government's Information Classification and Labelling Guidelines for delivery of Customer assets. The Customer will require security classification up to the "Unclassified" classification (or equivalent) set out in these guidelines.
- 5.12 From time to time, the Customer may re classify its data sensitivity levels and direct that the Contractor take specified steps or achieve specified types or levels of security, secrecy or privacy protection in respect of the Customer Data. The Customer and Contractor will review the reclassification of data requirement when it occurs and will confirm if any additional costs based on the Rate Card will apply.

## AUDIT REQUIREMENT

- 5.13** The Contractor must allow the Customer to conduct, or seek independent audits on the design and operating effectiveness of controls in the solution as they relate to the Customer's financial information and reporting to meet NSW Government policy and guidelines. TPP14-05 *Certifying the Effectiveness of Internal Controls Over Financial Information* requires that certifications comply with the requirements of relevant audit standards issued by the Audit and Assurance Standards Board (AASB), i.e.:

- ASAE 3000 *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*
- ASAE 3402 *Assurance Reports on Controls at a Service Organisation.*

A letter that provides assurance to NSW Treasury and the Audit Office of NSW will be the outcome of this audit requirement. There will be no additional cost on the Customer in the Contractor providing access to information required to meet these audit requirements.

## 6. Assumptions

### CUSTOMER RESPONSIBILITIES

#### Responsibility

#### SUPER USER GROUP

- 6.1** The Customer will be responsible for creating a Super User Group. Members of the Super User Group have a high degree of understanding of the Infor Workforce Management as a Service solution allowing them to add awards, change criteria, add users, change authorities as well as having a good understanding of the business processes being undertaken.
- 6.2** The Customer will ensure that the Super User Group:
- (a) are the primary contact point for the Contractor's support teams to assist in the triage / analysis of Incidents or Problems (for example providing detailed steps to recreate Incidents);
  - (b) track Incidents and escalate to Contractor as necessary;
  - (c) ensure that all available relevant details are provided to Contractor during escalation of a ticket;
  - (d) actively participate in high severity Incident resolutions as required to be a single point of contact for information to be provided to or by the Customer;
  - (e) help coordinate, along with Customer's Service Desk, communications about the Service including Incidents and Service Request related information, change and release coordination etc. to the system Users and other internal Customer business areas;
  - (f) deliver training and refresher training in relation to the application as required , provided that the Customer may request the Contractor to provide Training Services as an additional service;
  - (g) undertake or coordinate configuration of Customer related rules of software (eg awards and conditions),
  - (h) create requests for additional services to engage the Contractor to supply specific services – on the basis that a Super User will understand a business requirement and have the knowledge to determine how to best address the requirement ie either by completing the task inhouse or alternatively raising an additional Service Request with the Contractor,
  - (i) work with key Customer stakeholders to define requirements for any operational changes or enhancements required;
  - (j) help coordinate the timing and delivery of Acceptance Tests as requested by the Contractor;

- (k) manage Incident escalations with the Contractor's Infor Xtreme Portal; and
  - (l) schedule, monitor and approve system change requests as necessary.
- 6.3** The Customer will ensure that the Super User Group works closely with Permitted Users and the Contractor to address and close raised issues which are not Incidents including but not limited to:
- (a) business, policy and legislative related questions;
  - (b) questions with respect to the normal use and operation of the Services, such as 'how to' explanations;
  - (c) requests to add users;
  - (d) updates to user access (where such access is part of available, pre-defined profiles);
  - (e) communication with user groups during Infor Workforce Management System as a Service solution outages;
  - (f) issues related to the Customer's desktop standard operating environment, such as freezes, error messages, or slow performance within the Customers network; and
  - (g) user account administrative issues such as providing access at the appropriate levels, lockouts and password resets.
- 6.4** The Customer and the Contractor agree that they will work towards the objective of minimising the number of Level 1 Requests that the Contractor receives. The number of Level 1 Requests will be reviewed and managed through the appropriate Management Committee. The Level 1 functions are identified in the RACI chart included in Attachment 3-3 (Service Definition) to Schedule 3 (Service Level Agreement).
- 6.5** The Customer will use reasonable endeavours to ensure, through adequate training and resource planning, that it maintains a Super User Group of sufficient numbers with the ability to differentiate between Level 1 Requests and those to be allocated to the Contractor for resolution, as well as providing essential configuration services.

#### CONTRACTOR RESPONSIBILITIES

##### Service

Assumptions in relation to the Contractor's responsibilities in relation to the performance of this SLA are also defined in the Attachments to this Service Level Agreement.

## 7. Performance Measurement

- 7.1** The Contractor's performance will be measured against each of the defined Service Levels by the Customer for each full Measurement Period following Subscription Service Ready Date.
- 7.2** Performance measurement will be based on Service Level reporting and analysis information provided by the Contractor through the Infor Xtreme Portal, as well as actual information based on experience, retained by the Customer.
- 7.3** The Service Level Table sets out the Expected Service Level, Minimum Service Level, Measurement Period and other relevant information as applicable for each Service Level.

## 8. Payment Issues

#### PAYMENT SCHEDULE

- 8.1** The Contract Price is to be paid in accordance with Schedule 12 (PIPP) and Item 11 of the General Order Form.

#### AVAILABILITY SERVICE LEVEL

- 8.2** Availability is regarded as the Critical Service Level and as such, the following guidelines apply to the Availability Service Level apply:

- (a) Contractor will provide access to the WFM aaS solution (including interfaces) at Contractor's Internet gateway(s) twenty-four hours per day, seven days a week, except during Scheduled Maintenance.
- (b) Infor's service level objective is 99.5% availability for all components of the solution including interfaces.
- (c) Availability measured on a monthly basis.
- (d) Availability for the WFM aaS solution is measured monthly as a percentage of Scheduled Available Minutes where:
  - (i) "Scheduled Available Minutes" are the total minutes in a month less the number of Scheduled Maintenance minutes in the applicable month;
  - (ii) "Available Minutes" is the number of Scheduled Available Minutes in a month less the aggregate number of minutes the Services were unavailable outside of Scheduled Maintenance;
  - (iii) "Availability" is a percentage calculated as the Available Minutes in a month divided by the Scheduled Available Minutes in the month.

For example, in a 30 day month with 2 fortnightly Scheduled Maintenance windows of 4 hours per fortnight, there are 42,720 Scheduled Available Minutes ((60 min. x 24 hrs. x 30 days)-(60 min. x 4 hrs. x 2 weeks) = 42,720). If any module of the WFM aaS solution (including any interfaces eg IVR interface) experienced an outage of two hours outside of Schedule Maintenance, there were 42,600 Available Minutes in the month (42,720 Scheduled Available Minutes – 120 minutes of unavailability). The resulting Availability percentage is 42,600/42,720 = 99.7%.

#### EXCUSED PERFORMANCE

**8.3** The following shall not be considered periods of unavailability for purposes of the Availability calculation:

- (e) outages due to factors outside of Contractor's reasonable control (for example, a network or device failure at Customer's site or between Customer and Contractor's data centres);
- (b) delays in email or webmail transmission to or from the hosted application;
- (c) connectivity problems outside of Infor's direct control (e.g. DNS problems);
- (d) Events;
- (e) outages attributable to the acts or omissions of Customer or Customer's employees, agents, contractors, or vendors, or anyone gaining access to the services means of UserIDs or equipment controlled by Customer (other than those which are consistent with the proper use of the Services);
- (f) periods of down time at Customer's request;
- (g) outages that result from Customer's equipment, software, or other technology and/or third party equipment, software or other technology or services (other than those which are under Infor's direct control);
- (h) performance degradation due to Customer's use of the services in excess of the scope of Customer's license, usage restrictions, or product limitations outlined in the Contract;
- (i) Incidents for which the root cause analysis determines the cause to be outside of the scope of the Services provided by the Contractor; and
- (j) the Customer's operation of the Services otherwise than in accordance with applicable documentation or guidelines.

**'AVAILABILITY' DEFAULT AND SERVICE LEVEL CREDIT:**

**8.4** The following Rebates will apply should Availability fall below the nominated Service Levels as listed in the following table:

<u>Availability</u>	<u>Rebate</u>
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

**CONTRACTUAL REMEDIES**

**8.5** Where the Contractor does not meet the same Service Level in six (6) consecutive Measurement Periods, the Customer shall be entitled to treat such failure as a Substantial Breach for the purposes of clause 25.2 of the Customer Contract.

### Attachment 3-1: Service Level Requirements and Targets

Service Level Requirements and Targets	
<p><b>Contractor's Xtreme Portal and Xtreme Elite Support Service Levels</b></p>	
<p><b>Service Request Targets</b></p>	

Service Level Requirements and Targets						
Incident Response						
• See attachment 3-4 Support Services (Section 4 – Service Level Management Categories).						
Service Level	Minimum Service Level	Expected Service Level	Hours of operation	Critical or Key Service Level	Tolerance Limit	
<b>Incident Response</b>						

**Service Level Requirements and Targets**

[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
<p><b>Note: Measurement Period for Incident SLAs is monthly.</b></p> <p><b>Incident Severity Definitions are as follows:</b></p>							
<b>Level</b>	<b>Severity Definition</b>	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
Critical Incident Reviews	<ul style="list-style-type: none"> <li>• Critical Incident Reviews, including root cause analysis or applicable action plan, will be conducted on all Security Incidents within 5 Business Days (or as otherwise agreed) of resolution of the incident.</li> <li>• Critical Incident Review findings and mitigation strategies will be implemented to minimise likelihood of the same incident occurring in the future, will be included in monthly client reports.</li> </ul>	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]





<b>Service Level Requirements and Targets</b>		
█	█ █ █	█
<b>Backups, Restores, and Data Retention Requirements and Targets</b>		
█	█ █ █	█ █ █
█	█ █ █	█ █ █
█	█ █ █	█ █ █
█	█ █ █	█ █ █
<b>Audit Targets</b>		

Service Level Requirements and Targets		
	<ul style="list-style-type: none"> <li>█</li> <li>█</li> <li>█</li> <li>█</li> <li>█</li> </ul>	<ul style="list-style-type: none"> <li>█</li> <li>█</li> <li>█</li> <li>█</li> <li>█</li> </ul>
	<ul style="list-style-type: none"> <li>█</li> <li>█</li> <li>█</li> <li>█</li> <li>█</li> </ul>	<ul style="list-style-type: none"> <li>█</li> <li>█</li> <li>█</li> <li>█</li> <li>█</li> </ul>
Release Management Requirements		
	<ul style="list-style-type: none"> <li>█</li> <li>█</li> <li>█</li> <li>█</li> <li>█</li> </ul>	<ul style="list-style-type: none"> <li>█</li> <li>█</li> <li>█</li> <li>█</li> <li>█</li> </ul>
	<ul style="list-style-type: none"> <li>█</li> <li>█</li> <li>█</li> <li>█</li> <li>█</li> </ul>	<ul style="list-style-type: none"> <li>█</li> <li>█</li> <li>█</li> <li>█</li> <li>█</li> </ul>
Customer Satisfaction		
	<ul style="list-style-type: none"> <li>█</li> <li>█</li> <li>█</li> <li>█</li> <li>█</li> </ul>	<ul style="list-style-type: none"> <li>█</li> <li>█</li> <li>█</li> <li>█</li> <li>█</li> </ul>

## **Service Level Notes**

### **Xtreme Elite Support**

- (a) Incidents are to be logged by the Customer through use of the Contractor's Xtreme Portal or Infor Customer Care by phone if Xtreme Portal is off-line or where a Severity 1 issue has occurred.

### **Incident Resolution Service Level**

- (b) Time starts running once the Incident is either detected by the Contractor or is reported to the Contractor by a member of the Super User Group or any other personnel authorized by the Customer to make such reports. The Incident is logged immediately by the Customer into the Contractor's Xtreme Portal Management System where it will be tracked.
- (c) Resolution Time for all Incidents shall be measured from the time that the Incident is reported until the time of resolution of that Incident. The Contractor records and holds this information in the Infor Xtreme Portal.
- (d) The Severity level for each Incident shall be initially assigned by the Customer and recorded in the Contractor Xtreme Support Portal. This assignment will be reviewed and may be adjusted by Contractor with agreement from the Customer.
- (e) Where an Incident is downgraded to a lower Severity level, the measures for that lower Severity level shall apply to the entire Incident.
- (f) Where an Incident is upgraded to a higher Severity level, the measures for that higher Severity level shall apply from the time of upgrading the Incident.
- (g) Incidents shall be measured in the Measurement Period in which they are resolved. All open Incidents shall be included in the regular reporting so as to provide visibility to any Incidents that may be outside the Service Level.
- (h) Where multiple Incidents occur for the same event, those Incidents shall be aggregated and reported as the single first lodged Incident that relates to the issue.
- (i) Where a Service Level continues to fall below the minimum service level targets for a period of 6 or more consecutive months the failure to achieve the relevant Service Level will be deemed to be a Substantial Breach that is not capable of remedy.

## Attachment 3-2: Management Committees

### 1. Management Committees

- 1.1** This Attachment 3-2 (Management Committees) to Schedule 3 (Service Level Agreement) provides details on the structures and processes necessary to effectively manage the relationship between the Contractor and the Customer. Each committee established under this Attachment 3-2 (Management Committees) to Schedule 3 (Service Level Agreement) will be deemed to be a "Management Committee" for the purposes of Item 16 of the General Order Form and clauses 6.3 – 6.9 of the Customer Contract.
- 1.2** Clauses 6.3 – 6.9 of the Customer Contract will apply to each Management Committee established under this Attachment 3-2 (Management Committees) to Schedule 3 (Service Level Agreement).
- 1.3** The following levels of service delivery governance involving both Contractor and Customer are defined below:
- (a) management governance;
  - (b) operational service delivery governance;
  - (c) project governance.
- 1.4** Project governance is separate to the operational service delivery governance structure although there may be some overlap in membership representation. The Management Committee for project governance will be the "Infor Workforce Management System Project Steering Committee". The project governance structure will be used in the first instance for the Transition In Services, and the same governance structure will then be used for any subsequent projects. Project governance and relevant committee will only be required to meet when there are active projects.
- 1.5** The Management Committees to be established to support the above governance structure and to provide the appropriate Incident escalation structure will be as follows:
- (a) Management Committee;
  - (b) Operational Service Delivery Management Committee; and
  - (c) Project Steering Committee.
- The membership of each Management Committee and its functions are detailed in section 2 below.
- 1.6** The Contractor must establish each of the Management Committees required and both Parties must ensure that their relevant Personnel attend each Management Committee meeting.
- 1.7** The Management Committees may appoint and determine sub-committees to carry out any of its functions, provided that each sub-committee has appropriate representation from both Contractor and Customer
- 1.8** The Contractor and Customer may have additional internal committees to provide direction to organisational representatives of the above committees.

### 2. Governance Functions

- 2.1** The key governance bodies and functions are as detailed in the following table:

## PART 2: CUSTOMER CONTRACT

Governance Body	Meeting Frequency	Chaired By	Governance Functions	Members
<p>Management Committee (Contractor and Client Service Management Governance Forum)</p>	Annual	Customer	<ul style="list-style-type: none"> <li>• Conduct annual review of services and oversee the ongoing service delivery of the WFMaaS solution.</li> <li>• Contractor to advise Customer of any proposed changes to the WFMaaS solution pricing identifying contractual impact or price implications of such proposed changes.</li> <li>• Customer to advise Contractor of any intentions to increase or reduce services required (including providing notice of planned termination or transitioning out from the WFMaaS solution).</li> <li>• Discussion and approval to implement significant Updates, Upgrades, additional functionality or product changes and determine targeted timeframe.</li> <li>• Consult with Customer on annual schedule release dates and Outage calendar.</li> <li>• Review enrich and innovation opportunities.</li> <li>• Consider Customer feedback on potential future directions, enhancements or increased functionality requirements to feed into the future WFMaaS solution roadmap</li> <li>• Act as highest point of escalation to resolve Incidents or concerns affecting the Customer.</li> <li>• Approve contract variations.</li> </ul>	<ul style="list-style-type: none"> <li>• Contractor Executive Contract Manager</li> <li>• Deputy Commissioner, Offender Management and Operations</li> <li>• General Manager or Chief Superintendent, Operations Scheduling Unit</li> <li>• Customer CIO as Customer Contract Management Executive</li> <li>• Assistant Director BIMS</li> <li>• Assistant Director Infrastructure</li> <li>• Director Human Resources</li> <li>• CSNSW Custodial Representative (TBA)</li> </ul>
<p>Operational Service Delivery Management Committee (Service Delivery Operational)</p>	Quarterly	Customer	<ul style="list-style-type: none"> <li>• Review operational service delivery performance in line with the SLA and service delivery agreed performance levels and expectations and discuss opportunities for Service improvement.</li> <li>• Review service delivery reports including the Customer Satisfaction Survey and Critical Incident Reports.</li> </ul>	<ul style="list-style-type: none"> <li>• Contractor Service Delivery Manager</li> <li>• Customer Service Delivery Manager</li> </ul>

## PART 2: CUSTOMER CONTRACT

Governance Body	Meeting Frequency	Chaired By	Governance Functions	Members
Governance)  (Contractor and Client Business as Usual (BAU) Service Delivery Management Forum)			<ul style="list-style-type: none"> <li>• Customer to identify and advise of known peak periods or business critical periods.</li> <li>• Identify, manage and resolve Risks and issues associated with service delivery.</li> <li>• Review fees and invoices.</li> <li>• Review and determine any Rebates to be applied.</li> <li>• Manage and prioritise variations and Service Requests.</li> <li>• Raise and resolve issues or escalating issues where timely resolution not achievable.</li> <li>• Review report on all Security Incidents and make required decisions associated with mitigating similar future incidents.</li> <li>• Review any unplanned outages and resultant Critical Incident review reports.</li> <li>• Provide early advice on changes to Service delivery requirements or adoption of new functionality.</li> </ul>	
Service Delivery Management (Day to day Service Delivery Management)	As required	Contact by either party on needs basis	<ul style="list-style-type: none"> <li>• Day to day service delivery contract management of the Service.</li> <li>• Contact point to manage outage requests or changes to the approved Outage calendar including Emergency Planned Outages and Additional Planned Outages.</li> </ul>	<ul style="list-style-type: none"> <li>• Contractor Service Delivery Manager</li> <li>• Customer Service Delivery Manager</li> </ul>
(Contractor and Client Vendor Management Forum)				
Project Management Committee	Monthly	Customer	<ul style="list-style-type: none"> <li>• Provide overall management, direction and control of projects to ensure projects undertaken are delivered on time, within budget and that project delivery meets specified requirements.</li> </ul>	<ul style="list-style-type: none"> <li>• Contractor Project Executive Lead</li> <li>• Contractor Project</li> </ul>

## PART 2: CUSTOMER CONTRACT

Governance Body	Meeting Frequency	Chaired By	Governance Functions	Members
			<ul style="list-style-type: none"> <li>• Approve project plan.</li> <li>• Review progress against agreed project plans and Milestones.</li> <li>• Ensure that the Transition In and Schedule 12 (PIPP) are complied with, and that the Milestones are met.</li> <li>• Track, review and manage Risks relating to projects.</li> <li>• Oversee the project, including Acceptance Testing.</li> <li>• Review and manage project costs against approved budgets.</li> <li>• Review, approve/reject and prioritise change requests and variations within allocated budget.</li> <li>• Ensure resourcing meets needs to complete project satisfactorily on time and within budget.</li> <li>• Resolve project issues /disputes and provide direction, clarification or escalation where required.</li> <li>• Prioritise and re-prioritise project activities where required.</li> <li>• Provide direction and clarification as required.</li> <li>• Ensure appropriate change management, training and communication is in place.</li> <li>• Oversee the ongoing service delivery of the WFM aaS solution.</li> <li>• Review activities and delivery of Services against the Customer Contract.</li> <li>• Seek feedback from Customer and review Customer feedback register, to ensure customer expectations are being met or feedback is included in forward planning where necessary.</li> </ul>	<p>Manager</p> <ul style="list-style-type: none"> <li>• Customer Project Sponsor</li> <li>• Customer CIO</li> <li>• Customer WFS Project Manager</li> </ul>



## PART 2: CUSTOMER CONTRACT

Governance Body	Meeting Frequency	Chaired By	Governance Functions	Members
			<ul style="list-style-type: none"> <li>• Review performance against agreed Service Levels.</li> <li>• Customer to identify and advise of known peak periods or business critical periods.</li> <li>• Identify opportunities for Service improvement, new products or product innovation.</li> <li>• Review fees and invoices.</li> <li>• Review Rebates applied.</li> <li>• Communicate and consult with Customer on annual schedule release dates and Scheduled Maintenance calendar.</li> <li>• Manage Risks and issues associated with Service delivery.</li> <li>• Manage and prioritise variations and requests for additional work.</li> <li>• Resolve escalations referred by Operational Service Delivery Management Committee.</li> <li>• Identify changes in volumes or Customer requirements.</li> <li>• Review report on all Security Incidents and make required decisions associated with mitigating similar future incidents,</li> </ul>	

## Attachment 3-3: Service Definition

### 1. WFM System as a Service solution

#### SCOPE

- 1.1** The Infor Workforce Management System as a Service solution is to be delivered as a fully managed 'cloud service' for the Customer, with the Contractor responsible for the provision of all infrastructure (ie supply and hosting of the platform, and the Application software and interfaces (including IVR interface) (save for any Customer Supplied Items) required to make the Infor Workforce Management as a Service solution available remotely to Customer.
- 1.2** The following modules are included as part of the on-going operation of the WFM aaS solution as implemented in accordance with the Schedule 12 (PIPP):

	Component	Detail
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]
●	[REDACTED]	[REDACTED]

- 1.3** The Infor Workforce Management System as a Service solution is based on the implementation of commercial off the shelf software (COTS). Unless otherwise identified in Schedule 12 (PIPP), the scope will only implement standard, unmodified, functionality.
- 1.4** Should it be decided, based on the Customer's requirements and business processes, that extensions are required, support of such extensions would need to be purchased by the Customer for an additional fee in line with the established Customer Contract.
- 1.5** No custom extensions will be performed for the mobility module. If any functionality is identified that is not available in the core mobility product, then the business processes will be changed to follow the core functionality available or a product enhancement will be submitted for future consideration for mobility inclusion.

- 1.6 The Application will be configured in English only.
- 1.7 The Infor Workforce Management as a Service solution is provisioned for the Customer to support the organisational, functional scope described in Schedule 12 (PIPP).
- 1.8 The Infor Workforce Management as a Service solution will be implemented as detailed outlined in Schedule 12 (PIPP) to the specific needs of the Customer. The Service is based on a standard application with the capacity to personalise and adapt to Customer specific awards, workforce types conditions and other requirements, within pre-defined limits and an IVR interface.
- 1.9 The Infor Workforce Management System as a Service solution is based on the implementation of commercial off the shelf software (COTS) and as such only standard reports delivered with the software are included in scope.
- 1.10 The Infor Workforce Management Software as a Service solution can use the Contractor's "Workforce Management Performance Premium" or the Customer's Business Intelligence (BI) tool for reporting. Details of reports included in the Transition In Services are included in Schedule 12 (PIPP).

**APPLICATION OPERATIONAL DETAIL**

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**SOLUTION CURRENCY**

- 1.26 The Contractor may issue updates to the Infor Workforce Management System as a Service from time to time according to its development schedule, for which it maintains exclusive control. The Contractor is under no obligation under this Customer Contract to provide any Updates or Upgrades to the Service other than as specified in the Customer Contract. If the Contractor applies any Update or Upgrade to the Service according to its implementation schedule, the Contractor will not unreasonably delay implementing any Update or Upgrade for the Customer. The Contractor will make commercially reasonable attempts to update the Infor Workforce Management System as a Service only during Scheduled Maintenance.
  
- 1.27 The Contractor will make reasonable efforts to keep the Customer apprised of planned changes to the Service which include the removal of features or functionality and will provide at least 60 days' prior written notice of the proposed removal of any feature or functionality. No removal of any feature or functionality may occur without the Customer's prior written approval, unless it is necessary to remove such feature or functionality in order to address any legal or regulatory issue and the Contractor will endeavour to provide Customer as much prior written notice as commercially practicable. This clause does not limit the Contractor's obligation under clause 4.4 of Module 10 (As a Service).

- 1.28** The Service “bundles” of functionality cannot be diminished during the period of the contracts ie the Contractor cannot redefine the Infor Workforce Management System as a Service bundle and reduce the scope of the functionality offered or change bundles thereby resulting in the addition of cost to the Customer for the services originally contracted.
- 1.29** The Customer will undertake system configuration, in relation to their own awards, rosters and business detail to ensure business relevancy is maintained, within agreed limits.
- 1.30** The Contractor will be responsible for keeping the Infor Workforce Management System as a Service updated. All changes to the Infor Workforce Management System as a Service should be made in accordance with the Service Definition and the RACI.
- 1.31** The Customer is responsible for integration of WFM aaS solution with its own systems in the case of an Update or an Upgrade. The Customer may engage the Contractor to provide additional services with respect to any Update or Upgrade, and in that case the Customer is responsible for all costs associated with those additional services including system integration services, business process analysis, web development updates, any updates to integrations or any required data transformations.

#### PLATFORM CURRENCY

- 1.32** The Contractor will promptly implement any new releases relating to the WFM aaS solution where the release addresses a security risk or defect.
- 1.33** With respect to the operating system, the Contractor will apply security patches or updates supplied for the operating system or the relevant original equipment.

#### APPLICATION PACKS

- 1.34** The specific timing of all patching will be based on the agreed maintenance windows, urgency of the update and other operational issues, provided that security-related patches will be implemented promptly.

#### SOFTWARE CURRENCY

- 1.35** Licenced software included in the Infor Workforce Management as a Service Solution is detailed in Section 1.2 of this Attachment.
- 1.36** Any software licenses required for the Infor Workforce Management as a Service solution has been included as part of this Contract.
- 1.37** The Contractor will provision, manage and install the required software on the necessary platform.
- 1.38** The Customer will maintain an agreed PC SOE for the client side if required, and as published by the Contractor and amended from time to time with respect to the WFM aaS solution versions.
- 1.39** The Contractor will maintain the currency of the WFM aaS solution by supplying and implementing corrective patches, support packs and enhancement packs. The Contractor will also provide the following Services in respect of the WFM aaS solution:
  - (a) Emergency patching – this activity will be performed as and when required. Emergency patches may comprise of corrections, security and urgent legislative patches.
  - (b) Support packs. The Contractor will schedule to implement these packs when and if available. The Customer and Contractor will both carry out a simple suite of regression tests to investigate whether application of these packs have adversely impacted the service.

- (c) Enhancement packs - these packs will be prioritised for release based on importance and effort. Enhancements are typically scheduled for future releases.
  - (d) No major upgrade will be made to the WFM aaS solution, for the term of the Customer Contract unless otherwise agreed with the Customer.
- 1.40** Prior to making any changes to the Infor Workforce Management System as a Service solution (including applying patches, support packs or enhancement packs), the Customer and the Contractor will test the relevant changes in a test environment to ensure that the change will have no adverse effect on the Infor Workforce Management System as a Service solution or the Customer when implemented. If any change implemented by the Contractor has a material adverse effect on the Infor Workforce Management System as a Service solution, the Contractor will at the request of the Customer roll the relevant software back to the version or configuration that prevailed immediately prior to the relevant change being implemented.
- 1.41** The Customer will carry out its own Acceptance Tests to test and report to Contractor any impacts to its Service.
- 1.42** Third party software (not licensed to the Customer by Contractor or provided via the Cloud agreement) related Incidents will be the responsibility of the Customer. For the avoidance of doubt this means that any configuration / customisation of adapters within 3rd party systems will be the responsibility of the Customer.

#### PRODUCT INNOVATION

- 1.43** The Contractor shall maintain an WFM aaS solution innovation roadmap.
- 1.44** The Customer can provide input into the WFM aaS solution innovation roadmap through the Management Committee and through enhancement requests made using the Xtreme Portal.
- 1.45** The WFM aaS solution innovation roadmap will be based on tenants' feedback, current market needs and the expected future requirements of the product.
- 1.46** The Contractor shall have regard to the following factors when considering the **WFM aaS solution** innovation roadmap and priorities (the sequence is not reflective of the importance or weighting attached to each item):
- (a) requested functionality from the Customer. The Contractor retains sole discretion to include, or not include, functionality requested by the Customer;
  - (b) overall workforce management system market demand and direction;
  - (c) Risks associated with new solution components and the impact on the Customer;
  - (d) costs associated with the new functionality (implementation, support, Software licensing, infrastructure); and
  - (e) any other factors the Contractor considers would be beneficial to its Customers.

#### FEEDBACK PROCESS

- 1.47** The Contractor will ensure that the following items are included for consideration at the appropriate Management Committee meetings:
- (a) WFM aaS solution feedback;
  - (b) innovation feedback;
  - (c) results from an annual Customer Satisfaction Survey.
- 1.48** The Contractor will create and maintain a register of the Customer's feedback which will be used as input to the WFM aaS solution innovation roadmap.

- 1.49** The Contractor will consider the feedback from the Customer annually in the Management Committee.
- 1.50** The Contractor will comment on the Customer's registered feedback items at the Management Committee.
- 1.51** The Contractor will have the final decision on which innovations items will be implemented, the timing and manner of implementation.

#### **PRODUCT UPDATES**

- 1.52** Updates to the WFM aaS solution will be either:
- (a) mandatory, based on a change to the system (e.g. patching); or
  - (b) optional (e.g. new functionality). The Customer will have the option to accept or refuse any specific optional updates. Optional functional Updates that include bug fixes to existing functionality will be optional at no additional charge to the Customer. The Contractor will notify the Customer of any new functionality available for implementation.
- 1.53** For optional items (ie new Service functionality or components) that become available from time to time, the Contractor will notify the Customer if there are any Software licensing or other technical requirements for the Customer to receive the update.

#### **UPDATE IMPLEMENTATION PLAN**

- 1.54** In respect of any Updates to the Services, the Contractor will provide to the Customer an implementation plan which will specify the following:
- (a) the sequence, timing, dependencies and responsibilities for activities to implement the new functionality (if any) for the Customer; and
  - (b) the implementation plan will be developed based on the Transition In methodology described in Schedule 12 (PIPP) subject to any modifications required by the circumstances and the scale of the change.

#### **COMPUTE AND STORAGE CAPACITY**

- 1.55** The Contractor will provision sufficient compute resources to ensure satisfactory delivery of the WFM aaS solution.
- 1.56** The Contractor will provision suitable storage for the environments and landscapes in the scope of this WFM aaS solution.
- 1.57** The Contractor estimates that the storage estimates are sufficient to satisfy the Customer's requirements for the period of this contract and if insufficient the Contractor will provision additional capacity at no cost for the Customer.
- 1.58** The Contractor's storage services comprise:
- (a) provisioning, monitoring and management of the storage systems; and
  - (b) replication of production data to backup data centre to support disaster recovery,
- for the total solution, including any storage required relating to the IVR and other interfaces.
- 1.59** Should the Customer require an expansion of storage, as a result of a change in business scope or as a result of a significant increase in Permitted User numbers, the additional capacity will be allocated in line with services purchased and costed on the basis of pricing as per the Rate Card.

## INFRASTRUCTURE SERVICES

- 1.60** The Contractor will implement suitable monitoring tools for infrastructure monitoring, for application to monitor the WFM aaS solution on a 24 x 7 basis.
- 1.61** The Contractor will apply the necessary security features to ensure requirements in Section 5.8 of this SLA are met.

## BACKUP AND RECOVERY

- 1.62** The Contractor will provide the following backup and recovery features for Applications (including all interfaces) in accordance with the Service Levels:
- (a) primary and backup data centres ( backups stored off-site);
  - (b) backups include all operating systems and Customer Data; and
  - (c) backups will be encrypted using AES256 encryption.
- 1.63** With regards to backup management, the Contractor will perform the following services:
- (a) retention of daily and weekly production backups to cover a period of 46 days;
  - (b) retention of non-production backups for 14 days; and
  - (c) upon request, the Contractor will provide the Customer with a full data export of the Customer database.
- 1.64** Data restore requests, not resulting from any system failure or action by the Contractor, are regarded as an additional Service.

## NETWORK CONNECTIVITY

- 1.65** The WFM aaS solution will be provisioned within a secure Amazon Web Services (AWS) Virtual Private Cloud (VPC) network and the Customer will access the WFM aaS solution by using a public internet connection to the VPC. The Customer is responsible for configuration of all the required network devices (switching/routing/security) up to the WFM aaS solution point of presence.
- 1.66** The Customer is responsible for monitoring and management of network devices at their premises and for any infrastructure that is used to connect to the designated Customer's Amazon Web Services (AWS) Virtual Private Cloud (VPC) network.

## NETWORK CAPACITY

- 1.67** The Customer must provision sufficient network bandwidth up to the WFM aaS solution point of presence to access the WFM aaS solution. As part of the Initial Planning Stage (IPS), Infor will provide reasonable estimates of the bandwidth requirements to ensure satisfactory usability of the WFM aaS solution. The Contractor is required to advise the Customer of any sizing requirement changes following any product or usage changes, as part of the ongoing Service delivery.
- 1.68** The network capacity must be able to adequately service the peak loads in the application use. QOS should be implemented if required.

## CUSTOMER DEVICES:

- 1.69** The Customer will maintain all personal computers (PCs) and other client side infrastructure required for its personnel to access and use the WFM aaS solution as a remote server application.



- 1.70** The Customer will ensure currency of the PC SOE to ensure that implemented versions of the application can continue to be run effectively on its PCs.

#### **SUSPENSION**

- 1.71** The Contractor may not suspend the provision of any part of the Services to the Customer (or any of its Users), except and to the extent it is necessary to lock access of a Permitted User or terminate processes to address an identified risk to the use of the Services that:

- (a) poses a security risk to or may materially harm the Services or any third party; or
- (b) may adversely impact the services or systems,
- (a) provided that any such suspension must:
- (c) be in respect only of the relevant Permitted User and the minimum necessary portion of the Services;
- (d) not be in respect of more than a single Permitted User in relation to the identified risk without the prior consent of the Customer; and
- (e) be for only as long as reasonably necessary.

- 1.72** The Contractor will, where not prohibited by law and reasonable under the circumstances:

- (a) provide Customer with prior notice of any such suspension of Services; and
- (b) allow the Customer an opportunity to take steps to avoid any such suspension.

- 1.73** Upon any suspension of the Customer's or any Permitted User's right to access or use any portion or all of the Services and if the suspension is due to the fault of the Customer or such Permitted Users, then:

- (a) the Customer will continue to be liable to pay the usual fees for the Services during the period of suspension;
- (b) the Customer will be responsible for any applicable fees and charges for any Services to which Customer or any Permitted User continue to have access, as well as applicable data storage fees and charges, and fees and charges for in-process tasks completed after the date of suspension; and
- (c) the Customer will not be entitled to any Rebates under any Service Levels pertaining to any suspended Service.

- 1.74** If the suspension is not due to the fault of the Customer or any Permitted Users, the Customer will not be liable for any fees or charges relating to the suspended Services for the duration of the suspension.

## **2. Support Services**

#### **SERVICE LOCATIONS**

- 2.1** The Contractor's Support Services will be provided from locations in Australia and when needed, Contractor's global team will work on the Incidents logged to provide the support coverage as per the Infor Xtreme Elite Support plan. A general explanation of the Infor Xtreme Elite Support Plan is located at <http://www.infor.com/cloud/subscription/>

**SUPPORT SERVICES**

**2.2** The Contractor's Support Services are subject to the controls outlined in Attachment 3-4 (Support Services) and 3-5 (Security Services) to Schedule 3 (Service Level Agreement).

**APPLICATION SUPPORT SERVICES**

**2.3** The Contractors day to day operational responsibilities are summarised as follows and within the security framework as outlined in Section 5 and Attachment 3-5 (Security Services) to Schedule 3 (Service Level Agreement):

Service	High Level Service Summary
[REDACTED]	<ul style="list-style-type: none"><li>[REDACTED]</li><li>[REDACTED]</li><li>[REDACTED]</li><li>[REDACTED]</li><li>[REDACTED]</li><li>[REDACTED]</li></ul>
[REDACTED]	<ul style="list-style-type: none"><li>[REDACTED]</li><li>[REDACTED]</li><li>[REDACTED]</li></ul>
[REDACTED]	<ul style="list-style-type: none"><li>[REDACTED]</li><li>[REDACTED]</li><li>[REDACTED]</li><li>[REDACTED]</li><li>[REDACTED]</li><li>[REDACTED]</li><li>[REDACTED]</li><li>[REDACTED]</li><li>[REDACTED]</li><li>[REDACTED]</li><li>[REDACTED]</li><li>[REDACTED]</li><li>[REDACTED]</li><li>[REDACTED]</li></ul>

**SERVICE EXCLUSIONS**

**2.4** The following functions are out of scope for the Contractor as part of the ongoing Services of this Contract after the Subscription Service Ready Date, but may be considered, as available additional services with costs associated as detailed in Schedule 12 (PIPP):

- (a) level 1 Xtreme Elite Support Requests;
- (b) business process support and legislative support;

- (c) enhancements and changes that do not fall within definition of Service Requests and are not consistent with the WFM aaS solution roadmap;
- (d) Upgrades will be addressed through additional services and are not part of the standard Services;
- (e) Permitted User training will be addressed through additional services and are not part of the standard Services;
- (f) Customer site based services;
- (g) Customer LAN, desktop and PC SOE management;
- (h) Permitted User security – identity management;
- (i) steps required to reproduce the problem (Customer to provide); and
- (j) organisational change management.

#### DATA MIGRATION AND CONVERSION

- 2.5 Data migration and conversion relates to the efforts associated with the analysis, cleansing, transformation/mapping, loading and reconciling of current or historical data from other systems into the WFM aaS solution either manually or by use of programmatic methods. The data migration and conversion tasks are project related functions and are therefore detailed in Schedule 12 (PIPP):
- 2.6 The Contractor will work with the Customer in completing required integration on a needs basis, although primary responsibility for data migration remains with the Customer.

#### INTERFACES AND INTEGRATION

- 2.7 The Electronic Service Bus (ESB) required for interface and integration purposes (includes application platform, software and transformation services) will be supplied by the Customer or the Customer's nominated third party supplier.
- 2.8 The interface and integration solution will facilitate both 'real time' and 'batch integrations' as defined in Schedule 12 (PIPP) and agreed.
- 2.9 Interfaces and integration will be required for the IVR and to allow data to move either into or out of the installed applications, either in batch, real-time or near-real time. Interfaces are defined by the business processes they facilitate, the Contractor agreed processes, the points during those processes where data is exchanged, the frequency in which data is exchanged, and the method by which the data is exchanged.
- 2.10 Interface and integration points and requirements (including those for the IVR) are detailed in Schedule 12 (PIPP): Interface and integration requirements will be classified in three categories of complexity ie low, medium and high. and details associated with classification will be included in Schedule 12 (PIPP):
- 2.11 The Contractor will work with the Customer in completing required interface and integration on a needs basis, although primary responsibility for integration decisions and activities remains with the Customer.
- 2.12 All data files for outbound and inbound interfaces with Contractor applications will be in the specified Contractor standard file formats and will utilise .csv file types.
- 2.13 The Customer is responsible for defects arising from Customer Data.
- 2.14 The Customer will provide access to relevant environment, data, and systems to test interfaces for all Customer and third party systems to which the Contractor applications will be interfaced with including the IVR.
- 2.15 The Customer will be responsible for building the source system side of the interface, as required.

- 2.16 The Customer is responsible for data validation efforts associated with interface testing, ensuring interfaced data, including any transformation, mapping or aggregating logic, is performing correctly.
- 2.17 Should the complexity of any of the in-scope data migrations or conversions change in the Transition In Services, Contractor will work with Customer to address these changes using the Schedule 4 Variation Procedures.
- 2.18 The Contractor will provide rate details in the Rate Card so that the Customer may engage specialist integration staff if and when required.

#### **CHANGE MANAGEMENT AND TRAINING**

- 2.19 The Contractor will provide rate details in the Rate Card so that the Customer may engage Specialist Change Management and Training staff if and when required.
- 2.20 Change Management details, roles and responsibilities for the Transition In Services are covered in Schedule 12 (PIPP).
- 2.21 The Customer is responsible for user adoption & training efforts related to planning, designing, content development and delivering training to Permitted Users.
- 2.22 The Contractor will provide a third environment for the Customer's use for training and simulation purposes.
- 2.23 The Customer is responsible for providing business area subject matter experts to provide guidance/knowledge for the development of course material, and to participate in course material review cycles.
- 2.24 The Customer is responsible for all training delivery logistics. This is to include, but not limited to, enrolling and scheduling of trainees and trainers, printing and shipping of course materials, and obtainment and preparation of training facilities.

#### **SERVICE MANAGEMENT PROCESSES**

- 2.25 The Contractor is to have structured support services aligned to Contractor standard support processes.
- 2.26 Support Services are described in Attachment 3-4 (Support Service) to Schedule 3 (Service Level Agreement).

#### **BUSINESS CONTINGENCY**

- 2.27 The Contractor will develop a detailed Business Contingency Plan before the Subscription Service Ready Date as part of the Transition In Services, and will review and update this plan as new services and additional areas of the business are included. The Business Contingency Plan will comply with requirements as detailed in sections 4.6 to 4.12 of this SLA.

### 3. Services RACI Chart

#### DETAILED RESPONSIBILITY MATRIX

3.1 The key service delivery accountabilities for Contractor and Customer in relation to the WFM aaS solution and Support Services are defined in the following Service RACI chart:

Process - Service		Service Responsibility Matrix	
		Contractor	Customer
	<b>Level 0 - Management</b>		
<b>1</b>	<b>Management</b>		
1.01	Business contingency planning	R, A	C
1.02	Disaster Recovery planning for the WFM aaS solution	R, A	C
1.03	Project definition	C	R, A
1.04	Project approval	C	R, A
1.05	Manage centralised documentation	R, A	
1.06	Create and maintain documentation for procedures, services and operational activities for in-scope services	R, A	
1.07	Nominate contract managers to liaise, consult, support and provide authorisations to support procedure decisions	R, A	R, A
1.08	Develop, document and maintain client specific procedures relating to the WFM aaS solution		R, A
1.09	Provide Customer agency internal and external audit support (1 audit of up to 5 days included in base price).	R, A	C
1.10	Manage outputs and resolutions resulting from audit activities	C	R, A
	<b>Level 1 - Customer Service Desk</b>		
<b>2</b>	<b>Call Management</b>		
2.01	Call/Incident logging – via phone or web (dependent on severity)		R, A
2.02	First level case-based problem resolution		R,
2.03	Raise Incidents	I	R, A
2.04	Track Incident resolution and report to Permitted User on progress where appropriate		R, A
2.05	Escalate Incidents as necessary according to procedures	I	R, A
2.06	Close calls	I	R, A
2.07	Update internal knowledge base		R, A
2.08	Provide appropriate training (following completion of Transition In Services) to all Super Users and Customer's Service Desk personnel to support procedures, ensure correct triaging of calls and ensure competency		R, A

Process - Service		Service Responsibility Matrix	
		Contractor	Customer
	in use of service desk and help desk software		
2.09	Provide advice to Permitted Users on the functionality and in the use of general Customer applications and software		R, A
2.10	Provide appropriate training to WFM aaS solution users		R, A
<b>3</b>	<b>Incident Management</b>		
3.01	Operate Level 1 support desk		R, A
3.02	Provide support desk	R, A	
3.03	Log all Incidents into the appropriate Incident recording system	I	R, A
3.04	Raise alerts where system performance degradation to unacceptable levels is experienced	I	R, A
3.05	Provide and support Incident management system		R, A
3.06	Aim to close in scope Incidents on first contact		R, A
3.07	Track Incident resolution and report on progress		R, A
3.08	Escalate Incidents as necessary to partner providers according to procedures	I	R, A
3.09	Close calls	I	R, A
3.10	Track and report on number of calls that need to be reopened as considered unresolved to the Customer	R, A	C, I
3.11	Update internal knowledge base		R, A
3.12	Provide appropriate 1st level user support and training for WFM aaS solution.		R, A
3.13	Maintain printer profiles at application level		R, A
3.14	Provide Critical Incident Review reports for all Security Incidents within 5 Business Days of event resolution	R, A	I
	<b>Level 2 - Service and Support</b>		
<b>4</b>	<b>Incident Management (for all components of WFM aaS solution)</b>		
4.01	Level 2 Xtreme Portal - Incident logging	R,A	
4.02	Provide Xtreme Portal and Xtreme Elite Support Services for communication of tickets and status updates	R,A	
4.03	Provide and support Incident management system	R,A	
4.04	Advise Customer immediately if monitoring identifies system Problems	R, A	I
4.05	Advise Customer if Severity priority changed	R	I, C