Process - *Service*		Service Responsibility Matrix	
		Contractor	Customer
4.06	Aim to close in scope Incidents on first contact	R, A	I
4.07	Confirm receipt, track Incident resolution and report to Customer on progress. Response targets are detailed in Attachment 3-1 of this SLA	R, A	I
4.08	Diagnose and escalate Incidents as necessary according to procedures	R, A	
4.09	Produce and provide problem diagnosis information and trace files	R, A	
4.10	Close Incidents post confirmation from Customer	R, A	
4.11	Update internal knowledge base	R, A	
4.12	Provide Level 2 Incident support	R, A	
4.13	Escalate Incidents as necessary according to procedures	R, A	I
4.14	Determine Incident resolution or work-around solution	R, A	C
4.15	Implement Incident resolution or work-around solution	R, A	C
4.16	Verify Incident resolution	R, A	C
4.17	Coordinate with User for resolution as required, communicate resolution or work-around and close Incident		R, A
4.18	Undertake remedial action following critical business failure or unplanned outage and prepare critical Incident report to minimise likelihood of reoccurrence of similar Incident	R, A	I
4.19	Provide appropriate training to all users of the Contractor's Xtreme Portal in the agreed support procedures and Xtreme Portal software	R, A	
5	**Service Management**		
5.01	Participate in service and support activities and communications in line with SLA requirements including governance detail outlined in Attachment 3.2	R, A	C, R
5.02	Provide Service Level (based on this Schedule) reporting in accordance with Customer Contract	R, A	I
5.03	Management of the WFM aaS solution	R, A	R, A
6	**Batch (Application Batches)**		
6.01	Facilitate all Batch operations, including batch operation error correction and recovery	R, A	
6.02	Batch operations data correction		R, A
6.03	Apply data fixes to rectify data inconsistencies and errors		R, A

Process - *Service*		Service Responsibility Matrix	
		Contractor	Customer
	Level 2 - Infrastructure and Security		
7	**Infrastructure (Platform and Communications) and Security -** *(Level 2)*		
7.01	Management of solution 3rd party providers	R, A	
7.02	Performance management	R, A	I
7.03	Infrastructure (Platform) security management	R, A	I
7.04	Application security management	R, A	I
7.05	Develop and maintain Contractor security policies in line with Contractual obligations	R, A	C
7.06	Develop and maintain a Business Contingency Plan and procedures for WFM aaS solution	R, A	I
7.07	Execute disaster recovery tests in line with BCP requirements	R, A	I
7.08	Manage 3rd party provider contracts	R, A	
8	**Solution Management**		
8.01	Maintain inventory of all components of solution	R, A	
8.02	Monitor and detect availability and performance events for in-scope services	R, A	I
8.03	Ensure device configuration backups for in-scope devices are maintained	R, A	
8.04	Coordinate Incident resolution with other partners/providers as necessary	R, A	
8.06	Update and maintain WFM aaS solution documentation	R, A	
8.07	Management of Customer's network connectivity to enable access to the service		R, A
9	**Security Management**		
9.01	Create/maintain/disable user security profiles/roles and user parameters	C	R, A
9.02	Create/maintain/disable user groups		R, A
9.03	Define user request and approval procedures		R, A
9.04	Request creation or disablement of a user ID		R, A
9.05	Unlock locked users		R, A
9.06	Setup/reset initial passwords for user IDs		R, A
9.07	Maintain passwords of privileged user IDs		R, A
9.08	Maintain passwords of service administration accounts	R, A	
9.09	Perform application security audits	R	R, A
9.10	Report any detected breaches of security	R	C
9.11	Ensure appropriate security of data	R, A	

Process - *Service*		Service Responsibility Matrix	
		Contractor	Customer
10	**Infrastructure Administration & Support**		
10.01	Storage management	R, A	
10.02	Infrastructure hosting management for all components of WFM aaS solution	R, A	
10.03	Develop and maintain instance/client configuration documentation	R, A	
10.04	Maintain specific Customer configuration detail documentation where configurations are undertaken by Customer		R, A
10.05	Troubleshoot infrastructure problems	R, A	
10.06	Apply patches, Updates and Upgrades (VM, O/S)	R, A	I
10.07	Ensure adequate system testing of all Application changes from a functional and user perspective (includes IVR and other interfaces)		R, C
10.08	Ensure adequate system testing of all Application changes from a technical perspective	R, C	
10.09	Create additional environments when required (additional costs apply)	R, A	C
11	**Equipment Maintenance (including servers)**		
11.01	Manage all 3rd party partnership to ensure Contractor's ability to provide services at the agreed levels for the duration of the contract	R, A	
	Level 2 - Operations		
12	**Operations Management**		
12.01	Coordinate and oversee daily operational activities required to fulfil contracted service levels.	R, A	
12.02	Maintain inventory of in scope application software, data bases and partners providing infrastructure platform hosting services	R, A	
12.03	Identify Customer licence requirements for WFM aaS solution	C	R, A
12.04	Ensure Customer licencing compliance based on requirements identified by Contractor	C	R, A
12.05	Undertake upgrades as approved by the Customer	R, A	C
13	**Operational Procedures** (managed by Infor)		
13.01	Ensure all necessary database activities are performed (eg imports/exports; investigation of Incidents and Problems; management of table space; database profile modifications etc)	R, A	

Process - *Service*		Service Responsibility Matrix	
		Contractor	Customer
13.02	Ensure all scheduled and ad hoc startup/shutdown of OS, hardware and applications are performed	R, A	
14	**Backup/Restore Management (O/S or Server)**		
14.01	Perform complete backups	R, A	
14.02	Restore complete or incremental backup as needed after system failures	R, A	
14.03	Validate integrity and consistency of restored information	R, A	
14.04	Test backup/restore procedures periodically	R, A	I
15	**Application Administration**		
15.01	Troubleshoot application problems	R, A	
15.02	Identify and proposed application software updates to be applied	R, A	
15.03	Perform application software updates	R, A	
15.04	Apply minor configuration and break fix modifications	R, A	
15.05	Monitor application availability	R, A	I
15.06	Perform application user administration procedures		R, A
	Level 2 - End to End Management		
16	**End to End Diagnosis**		
16.01	Diagnose production issues related to the end to end transactions serviced by the application including interfaces	R, A	C, I
16.02	Diagnose production issues related to the infrastructure used by the application including interfaces	R, A	I
16.03	Diagnose production issues related to the data stored in the application including interfaces	R, A	I
17	**IT Disaster Recovery**		
17.01	Maintain application disaster recovery plan and procedures	R, A	C I
17.02	Execute application disaster recovery tests in accordance with contract	R, A	I
18	**Capacity Planning**		
18.01	Ensure appropriate system capacity (database, server and storage) for the WFM aaS solution	R, A	
	Level 3 - Application		
19	**Service Request Management**		
19.01	Coordinate request approval	I	R, A
19.02	Manage daily activities and communications	R, A	R, A

Process - *Service*		Service Responsibility Matrix	
		Contractor	Customer
19.03	Estimate time and costs for additional Service Requests and High Priority Service Requests	R, A	C, I
19.04	Ensure delivery and implementation of all Service Requests (including High Priority Service Requests) and additional services at required standard and within negotiated and agreed timeframes.	R, A	R, A
20	**Applications Support**		
20.01	Configuration of application detail ie awards, conditions etc		R, A
20.02	Testing of configuration changes implemented as per 20.01		R, A
20.03	Maintaining documentation associated with configuration detail and changes made as per 20.01		R, A
20.04	Support Incident management process with root cause analysis	R, A	I
20.05	Manage and update centralised documentation on a timely basis	R, A	
20.06	Integration / interfaces between WFM aaS solution and Customer's retained applications systems in so far as this is not included as an additional service	R, A	C, I
21	**Configuration Management / Change Management**		
21.01	Define change management requirements	R, A	C, I
21.02	Define configuration management requirements	R, A	I
21.03	Execute agreed change management processes	R, A	C, I
21.04	Execute agreed configuration management processes (including notification to Super Users)	R, A	I
21.05	Notification of changes to Permitted Users		R, A
21.06	Maintain configuration documentation for all components of the WFM aaS solution back-end to an agreed standard and format	R, A	
21.07	Maintain electronic records of software configuration. Including versions. Modules and patches applied for all WFM aaS solution environments	R, A	
21.08	Undertake organisational change management for WFM aaS solution	C	R, A
22	**Application Performance and Tuning for applications supported by Contractor or Contractor 3rd parties**		

Process - *Service*		Service Responsibility Matrix	
		Contractor	**Customer**
22.01	Monitor, identify and manage application performance improvement opportunities from support cases, production monitoring or issue diagnosis	R, A	I
22.02	Monitor, identify and manage database performance improvement opportunities from support cases, production monitoring or issue diagnosis	R, A	I
22.03	Configure tuneable infrastructure parameters	R, A	
23	**Integration and Interfaces**		
23.01	Supply, monitor and manage an appropriate Interface and Integration solution	I	R, A
23.02	Determine Interface and Integration requirements (including source systems and environments).	I	R
23.03	Ensure appropriate security associated with the Interface and Integration platform		R
23.04	Completion of ETL functions		R
23.05	Resolution of Interface and Integration errors	C, I	R
23.06	Ensure licencing compliance associated with Interface and Integration solution	C, I	R
23.07	Maintain interface and integration documentation	I	R

Attachment 3-4: Support Services

1. Support Services (Overview)

PROVISION OF SUPPORT SERVICES

1.1 With respect to the Services, the Contractor will provide Support Services in accordance with this Attachment 3-4 (Support Services) to Schedule 3 (Service Level Agreement), the Service Levels set out in the Service Level Table, the security Services outlined in Section 5 of the Service Level Agreement and Attachment 3-5 (Security Services) to Schedule 3 (Service Level Agreement), and the Transition Out Services as outlined in Attachment 3-7 (Transition Out Services) for the duration of the Contract Period. The Support Services are included in the Contract Price.

LEVELS OF SUPPORT SERVICES

1.2 The Contractor's responsibilities:

(a) The Contractor's responsibilities are to support the operation and maintenance of all components of the Infor Workforce Management System as a Service solution.

(b) The Support Services will be provided by the Contractor's Personnel with suitable knowledge of and experience in the technical support appropriate to, and maintenance of, the Services.

(c) Where there is an Incident, the Contractor acknowledges that urgency and emphasis will, as applicable, be in priority of:

(i) traffic restoration;

(ii) Incident resolution;

(iii) performance affirmation;

(iv) IVR interface restoration or normalisation;

(v) network restoration or normalisation; and

(vi) investigation and root cause analysis of Problems and development of mitigation strategies to minimize the risk of any Severity 1, Severity 2 or Security Incidents re-occurring in the future.

(d) Support Services provided by the Contractor will include:

(i) An Xtreme Portal, as set out in Section 2 of this Attachment;

(ii) a Service Request service and a High Priority Service Request service, as set out in Section 3 of this Attachment.

1.3 Incident escalation

(a) The Customer, within its ability, will attempt to solve any Incident using the resolution procedures (if any) set out in the User Documentation.

(b) If the Customer is unable to solve an Incident, then the Customer will report the Incident to the Contractor by means of the Xtreme Portal and both parties will act in accordance with the standard escalation procedure below:

(i) most Incidents are best resolved through Contractor's standard operating procedures. If the Customer believes that a particular Incident requires a higher level of attention, the Customer should contact the regional Xtreme Support Center and request that a support manager become involved. Escalation or routing of Incidents

outside of standard procedures is reserved for Incidents/Problems that warrant a higher degree of attention, and such escalation is not appropriate for all Incidentss.

(ii) If escalation is requested, merited, Contractor will notify the appropriate support manager. The support manager will act promptly to assess the situation, contact the Customer to discuss a resolution plan, identify required resources, and implement the agreed upon resolution plan.

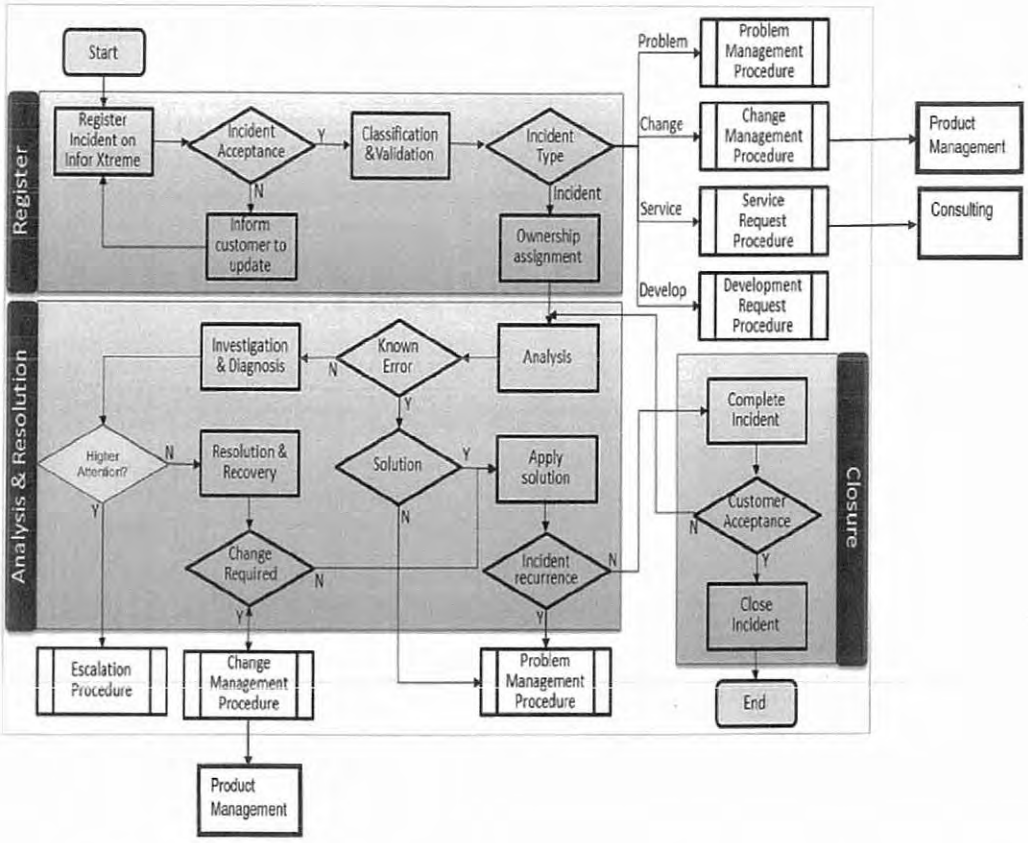
1.4 The Customer will use reasonable business judgment to identify the severity of the Support incident according to the following severity level descriptions:

Level	Severity Definition
Severity 1 – Critical	Severity 1 – CRITICAL - Production Down. A customer's production system, database or software is inoperable. A major application failure has occurred or data integrity issues exist, and business processes are halted. There is no workaround available. Severity 1 Incidents that occur after standard Xtreme Elite Support hours must be reported by telephone.
Severity 2 – High	Severity 2 – HIGH. A critical business process is impaired, causing a serious disruption of a major business function. It is causing serious impact on daily functions or processing, and there is no acceptable workaround.
Severity 3 – Medium	Severity 3 – MEDIUM. Non-critical problems occur with the software. Customer is able to run the system and/or application, and there is an acceptable workaround for the problem.
Severity 4 - Low	Severity 4 – LOW. An inquiry and/or low system impact issue which does not require immediate attention. This includes cosmetic issues on screens, errors in documentation, or a request regarding the use of the software.
	Note: Any type of Customer request that does not relate to a Defect is not an Incident.`
Severity 5 – Suggestion for Enhancement	Suggestion for Enhancement. A suggestion is made for enhancing the Subscription Software by adding new features or improving existing features.

1.5 The Support Services model will be based on the Infor Xtreme Elite Support model as confirmed in this Customer Contract.

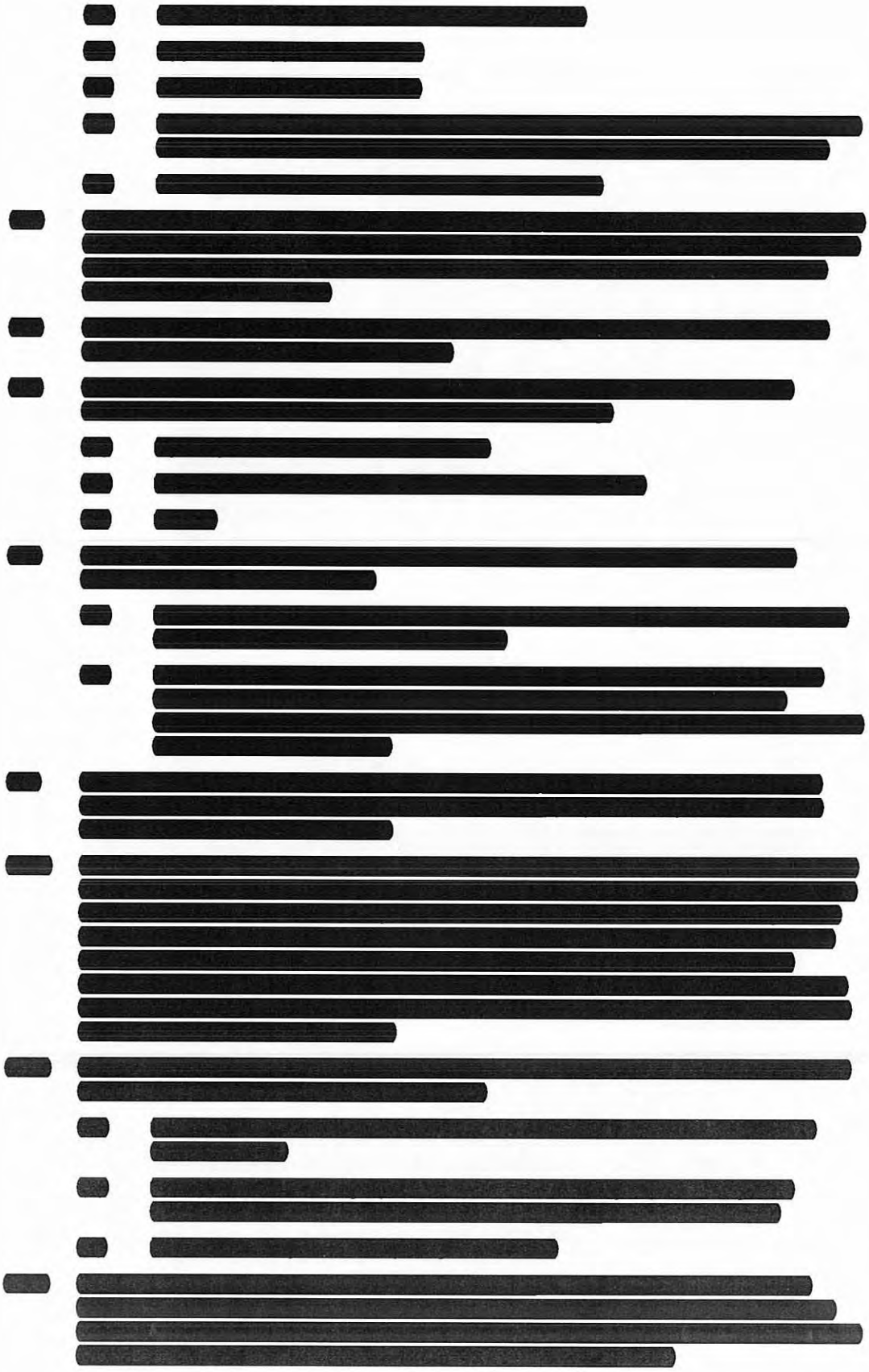
SERVICE DELIVERY MODEL

1.6 The diagram below illustrates the delivery model for the Support Services and points of interaction with the Customer's service management personnel.



2. Xtreme Elite Support Service (See Service Level Table – SLA-01)

[redacted]



[redacted]

[redacted]

3. Additional Service Requests (See Service Level Table – SLA-02)

3.1 This Contract allows for Service Requests relating to the Infor WFM System aaS solution. Service Requests are typically requests from the Customer for consulting work that are not Incidents.

3.2 There is no maximum period of days effort allowed for Service Requests.

3.3 An Service Request is to be assessed in accordance with Schedule 4 (Variation Procedures).

3.4 The Customer's authorised representatives may use the Xtreme Portal to lodge a Service Request at any time.

ADDITIONAL SERVICE REQUEST MANAGEMENT PROCESS

3.5 The Contractor will manage Service Requests as a queue of prioritized requests for one time Services. Service Request priority will be based on a forward demand planning arrangement with delivery dates mutually agreed by Contractor and the Customer subject to the availability of appropriate skilled resources by role/skill. The parties may agree to reprioritise Service Requests to take into account urgent matters.

3.6 The process for dealing with High Priority Requests and Incidents is detailed in Attachment 3-7 (Request Handling for High Priority Requests and Incidents) of Schedule 3 (Service Level Agreement).

3.7 Service Requests may include, but are not limited to:

(a) incremental processes or process options;

(b) new reports, different versions of reports;

(c) new enhancements;

(d) new forms, different versions of forms;

(e) new workflows; and

(f) new interface requirements.

3.8 The Contractor will track consumed and remaining hours for each Service Request and report on these to the Customer on a monthly basis. The Customer will be responsible for managing business demand in line with Service Request capacity available.

3.9 The Contractor will provide sufficient resources to undertake the Service Request capacity within an agreed time period.

4. Service Level Management Categories

4.1 The Customer will notify the Contractor, via the Infor Xtreme Portal, of any Incident with the WFM aaS solution. At that time, the Customer will advise the Contractor of the Severity category assigned to such Incident, which the Customer must reasonably

determine in accordance with the Incident severity definitions set out in the Service Level Table.

4.2 Both the Contractor's Personnel receiving the call and the Customer's Personnel reporting the Incident will agree on the time of the call (to the nearest minute) and will record that time.

4.3 Any request that is not in scope of an Additional Service Request or a 'High Priority Service Request or Incident' will be logged in accordance with the demand management process.

5. Incident Resolution (See Service Level Table – SLA-03)

5.1 On receipt of an Incident being logged by the Customer to the Infor Xtreme Portal, the Contractor must resolve the Incident in accordance with the Service Level Table.

5.2 The Contractor is not permitted to use a correction process to correct an Incident if:

(a) the correction process will result in the Services becoming unusable (or its performance becoming degraded) for more than a length of time to be agreeable to the Customer on any one occasion, such time to be agreed prior to the commencement of any correction process; or

(b) the correction will require the Customer to upgrade any of the software that is used, or that the Customer uses, with the Services unless there is no other way to resolve or correct the Incident.

DATA CORRUPTION

5.3 If an Incident (other than an incident resulting from Customer configuration or data entry activities) causes any corruption of Customer Data, then the Contractor must either:

(a) work with the Customer to determine the best way to correct the data corruption

(b) if agreed by both parties, that the Contractor is unable to comply with section 5.3(a) in a reasonable time, the Contractor will employ sufficient technical and/or data entry Personnel to re-construct and/or re-enter data as needed to correct the corruption.

6. Xtreme Elite Support Service Interface Procedure

[redacted]

Attachment 3-5: Security Services

1. Overview

1.1 The Contractor will maintain the security standards and data protection protocols outlined in this Attachment and Customer will undertake its responsibilities as detailed herein.

1.2 This Attachment 3-5 (Security Services) to Schedule 3 (Service Level Agreement) applies to the protection of Customer Data. Section 2 details frameworks and standards applicable to the Services. Section 3 details the protocols with respect to delivery of Support Services and section 4 the features implemented for the Infor Workforce Management System as a Service solution itself.

2. Security standards and control

STANDARDS

2.1 The Infor Workforce Management System as a Service solution is governed by the following security frameworks and industry standards:

(a) Contractor's client data protection program – which requires Contractor to implement the data protection controls outlined below; and

(b) Conforms to ISO 27001:2013. The Contractor is to ensure that the Infor Workforce Management System as a Service is included in the defined scope of the ISO certification.

2.2 With respect to the Subcontractors:

(a) The Contractor is required to manage all third party external Subcontractors engaged by the Contractor to support the Services and will adhere to all obligations of this contract. The Contractor will need to notify the Customer of all Subcontractors confirming their security compliance.

AUDIT & COMPLIANCE CONTROLS

2.3 The Contractor will undertake an annual audit in compliance with SSAE 16 SOC 1 or such other versions for which the Contractor is certified and will retain records pertaining to the same.

2.4 In accordance with the Contractor's customer data protection program, the Contractor will review its controls annually.

2.5 The Contractor will provide the Customer with a copy of the annual security compliance audit results.

2.6 The Customer will have the right to have one (1) independent security audit per annum of controls performed, provided the Contractor has a minimum of two 2 weeks' notice. Expenses for the audit will be covered by each party for their direct expenses.

2.7 In accordance with the Contractor's customer data protection program, the Contractor will review its controls annually.

2.8 The Contractor will maintain documentation for:

(a) certification as outlined in section 2.1(b) of this Attachment;

(b) data backups and restores;

(c) disaster recovery plan;

(d) Business Contingency Plan;

(e) security incidents reports and responses; and

(f) personnel security policies and procedures.

3. Data Protection Protocols

3.1 These data protection protocols set forth the procedures that Contractor will follow with respect to maintaining the security and privacy of Customer Data in connection with this Service Level Agreement.

SECURITY POLICY

3.2 The Contractor will maintain applicable policies, standards, and procedures intended to protect Customer Data consisting of:

(a) system security (for all components of the system), including but not limited to the following: Information Security Policy; Identification and Authentication Standards, Logging and Monitoring Standards approved encryption standards and products;

(b) security of information and Acceptable Use Terms;

(c) confidentiality obligations; and

(d) data privacy obligations as they pertain to NSW Government.

GLOBAL ACCESS

3.3 The Customer Data is to remain in Australia where possible and should be accessed only by staff of the Contractor in Australia unless when remote access to the Customer Data for support and maintenance purposes is required to deliver the Service Level(s) at which time access is available to the Contractor's global support team. Remote access and confidentiality of data will be in strict accordance and governed by the Contractor's Security and Data Privacy policies, practices and protocols at all times throughout the tenure of the Agreement.

ORGANISING INFORMATION SECURITY

3.4 The Customer and the Contractor will each appoint data protection executives who will be accountable for confirming the implementation of, and ongoing compliance with these procedures. Communication under these procedures will be as follows:

(a) communications regarding the day-to-day obligations should be communicated in writing via e-mail or other Notice in Writing to each of the data protection executives; and

(b) communications regarding any non-material change to the terms of these procedures should be provided as required under the notice provisions of the Customer Contract with copies provided to the data protection executives.

3.5 Any material changes to these procedures will be in accordance with Schedule 4 (Variation Procedures).

3.6 The data protection executives will jointly review these procedures at a minimum on an annual basis to identify if any changes are necessary. Each party will promptly notify the other party of any suggested changes to the application of agreed procedures or other general concerns about potential gaps in the information security environment.

HUMAN RESOURCES SECURITY

3.7 The Contractor shall ensure that Personnel involved in the provision of the Infor Workforce Management as a Service are:

(a) required to complete standard data protection training;

(b) subjected to appropriate background checks; and

(a) subject to terms of engagement that require them to comply with Contractor's relevant security policies and processes.

3.8 The Contractor will ensure that terms of employment for all employees and the Subcontractor's employees contain clauses addressing compliance with Contractor security policies.

3.9 The Contractor Personnel must undergo periodic security awareness training focused on essential security policies and emphasising the user responsibilities related to Incident management, data privacy and information security.

PHYSICAL AND ENVIRONMENTAL SECURITY

3.10 The Contractor will implement security controls as per the location security standard (as described in the section entitled "Support Locations" below) where Customer Data is being processed.

DATA CENTRE LOCATIONS

3.11 The Contractor will implement the following physical security features at all data centres:

(a) restricted access to Contractor owned/controlled data centres as follows:

(i) entrance barriers to control vehicle entry;

(ii) revolving access doors with personnel security trap; and

(iii) door access controls on all technical areas; and

(b) electronic access control and CCTV at entry/exit points and prominent locations, monitored 24x7. This includes:

(i) full coverage of exterior, entryways, lifts, stairs and site interior;

(ii) access control system for entrance, exit and lifts; and

(iii) individual pin lockable racks as standard.

SUPPORT LOCATIONS

3.12 Where Services are provided from Customer locations, the Customer's policies with respect to security will apply.

3.13 With respect to Contractor Personnel providing the Support Services located off shore, the following additional security measures will apply:

(a) facilities will have the following levels of security which are cumulative, listed in increasing order of stringency and will limit access granted to Contractor Personnel based on the facility access they require to complete their function:

(i) Level 0 – access to building premises (controlled by security guards);

(ii) Level 1 – access to reception lobby (controlled by security guards and/or access control); and

(iii) Level 2 – access to open work areas (controlled by access control readers);

(b) a combination of physical and electronic access control and surveillance including security guards, electronic access control monitored 24 hours, 7 days a week;

(c) all Personnel on-site shall be registered and required to carry appropriate identification badges;

(d) visitors to the sites will be required to be sponsored, will be issued with a visitors' identification badge and will be escorted when within the facility;

(e) facilities will have required infrastructure support with power backups using Uninterrupted Power Supply (**UPS**) and / or diesel generators to support critical services;

(f) all locations will be compliant with local safety laws including fire safety laws and Work Health & Safety (or equivalent) laws;

(g) the Contractor will operate the a 24/7/365 single point for all Contractor Personnel to report safety and security concerns; and

(h) the Contractor will have senior professionals dedicated to safety and security roles who will use various forums including regularly scheduled knowledge sharing exercises with support staff who are responsible for safety and security duties.

COMMUNICATION AND OPERATIONS MANAGEMENT

3.14 The Customer will be responsible for the communications and operations management security setting for Customer's own workstations, servers and network equipment.

3.15 The Contractor is required to implement a minimum set of hardening requirements (steps to lock down technology) for its technology infrastructure which includes workstations, servers and network equipment. Workstation / servers images will contain pre-hardened operating systems. Hardening requirements vary depending on the type of operating system and the applicable controls that are implemented. The key hardening controls to be used by the Contractor will be:

(a) services that are provided by default and not required for delivery of the Infor Workforce Management System as a Service solution such as telnet, remote registry and routing will be disabled;

(b) password policy implementation as per the Contractor's identification and authentication standards;

(c) screensaver configuration for auto lockout - a password protected screensaver will be invoked after 10 minutes of inactivity;

(d) default IDs will be disabled / renamed;

(e) access privileges will be assigned on the basis of the principle of "least privilege" (i.e. on an as needed basis with the default being access is not given to an individual unless their role specifically requires such access);

(f) logging and time synchronisation will be enabled;

(g) logon banner can be enabled; and

(h) security tools as applicable can be installed such as antivirus, personal firewall and encryption.

3.16 The Contractor's Support Locations are to install a suitable End Point protection on workstations. The servers are also to be protected using Microsoft a suitable security product such as Microsoft Forefront Endpoint Protection, McAfee or Symantec. Contractor's e-mail gateways are also to utilise a suitable security product to scan for potential virus/malware attachments (other than in respect of Hosting Providers, the requirements for which are set out in section 3.53 below).

3.17 The Contractor's internal network (excluding the specific Service network the requirements for which are set out in section 4 below) is required to have multiple layers of security built into its architecture to support resiliency and security. Access between Contractor's internal network, external networks and the internet is governed by defined inbound and outbound access policies placed on a combination of internal and external firewalls. Contractor firewalls are to be configured for "security by

default" (i.e. deny-all) policies. Key network security controls to be implemented are as follows:

(a) critical network zones are to be logically isolated. Systems with external connections will be protected by hardening and firewalls. Externally facing systems will be placed in a "Demilitarised Zone" (DMZ) or other similar configuration to protect internal Contractor systems;

(b) remote access to devices on the Contractor internal network, with the exception of the email system, requires the use of secure VPN solution;

(c) access control lists are to be implemented on perimeter / screen routers; and

(d) network intrusion detection / prevention systems (NIDS/ NIPS) are to be placed in strategic locations in the network and are to be monitored and managed 24 hours a day, 7 days a week.

3.18 Backup copies of essential information and configuration files are to be taken on a regular basis. Backups are to be encrypted with industry standard encryption when stored on portable media or transmitted outside of the Contractor's managed data centres.

3.19 The Customer and the Contractor require that sensitive information stored in an external / portable storage media be encrypted using approved encryption solutions.

3.20 The Contractor security policies and standards are to mandate only secure disposal of media. Contractor desktops and laptops are to be encrypted thus preventing the removal of data by unauthorised Personnel.

3.21 All devices that have logging capabilities, such as operating systems, databases, applications, firewalls, routers and switches are required to be appropriately configured to ensure security standards are maintained.

ASSET MANAGEMENT

3.22 The Contractor is required to implement processes to account for and manage software and hardware assets. Assets are required to have an identified owner for establishing the requisite security for that asset. Asset inventory agent software is required to be installed on all Contractor workstations, servers and network devices at Contractor locations.

3.23 The Contractor will comply with Customer-provided guidelines and policies in respect of Customer-provided devices.

INFORMATION CLASSIFICATION

3.24 The Contractor will utilise the NSW Government's Information Classification and Labelling Guidelines in delivery of Customer assets. The Customer will require security classification up to the "Unclassified" classification (or equivalent) set out in these guidelines.

NETWORK SECURITY MANAGEMENT

3.25 The Contractor will maintain access control lists for network devices.

3.26 Network traffic shall pass through firewalls that are monitored and protected by intrusion detection/prevention systems that allow traffic flowing through the firewalls to be logged.

3.27 Access to network devices for administration shall require industry standard encryption.

3.28 Anti-spoofing filters shall be enabled.

3.29 Network, application, and server authentication passwords will meet each party's complexity guidelines.

3.30 To the extent possible, the Customer will disable non-Customer email access from Customer-provided devices that access Customer Data.

VIRTUAL PRIVATE NETWORKS

3.31 Connections will be encrypted using industry standard encryption.

MEDIA HANDLING WHEN TRANSFERRING CUSTOMER DATA

3.32 Both the Contractor and the Customer will implement encryption of Customer Data where required unless restricted by local regulations or agreed by both parties. The Contractor will set up secure connectivity from its support locations to each of the data centres for the Infor Workforce Management System as a Service solution using site-to-site VPN tunnels with appropriate level of encryption.

3.33 Use of portable media to transfer Customer Data will be avoided if possible. When necessary, transfers of data on recordable or portable media must be encrypted at all times while in transit, with encryption keys transported or transmitted separately and all Customer Data transmitted between the parties will be conveyed using a secured and encrypted storage device or file transfer mechanism as agreed by the data protection executives. Portable backup media, e.g. tapes, DVDs/CDs, USB Flash ("Thumb") drives, etc. must be encrypted using Advanced Encryption Standard (AES) 256-bit encryption.

3.34 During the Transition In Services the Customer shall implement means such as masking or de-identification of personal information prior to providing access to Contractor or give permission to the Contractor to utilise unmasked data.

3.35 The Customer must identify instances where unmasked/unscrambled production data is used outside of production environments before providing Contractor access. If production data is used for testing, compensating controls shall be agreed and employed.

3.36 Sensitive data must not be copied into the development and test environments without the written approval of the Customer, and if used, must be treated in accordance with its classification.

DATA DISPOSAL

3.37 The Contractor will ensure that project or operational team members will return or destroy any Customer Data that is in their possession as soon as the Customer Data is no longer required for the immediate performance of the Services.

3.38 The Contractor may retain archival copies of records containing Customer Data as reasonably necessary or as part of normal business management processes to verify Contractor's compliance with this Agreement.

3.39 The Contractor shall destroy hard copies containing Customer Data via shredder or by depositing in a secure destruction bin when no longer required in the performance of the Services.

THIRD PARTY SERVICE DELIVERY MANAGEMENT

3.40 The Contractor will execute substantially similar contractual terms relating to privacy and security with all Subcontractors.

ACCESS CONTROL

3.41 The Contractor will apply the following principles to its own systems to control the access for Contractor Personnel to Customer Data:

(a) the principle of role based access is used for providing logical access control. User access is provided via a unique user ID and password. Contractor password policy has defined complexity, strength, validity and password history related controls;

(b) user account creation and deletion procedures as have been mutually agreed are implemented, for granting and revoking access to Customer systems that are used during the course of any project or as part of the ongoing service delivery contract;

(c) access rights are reviewed on a periodic basis; and

(d) Personnel ending their employment or affiliation with the Contractor will have their access revoked prior to or immediately on their departure.

3.42 The Contractor shall revoke access for Personnel departing the engagement as soon as reasonably practicable, or in compliance with contractual obligations, whichever is sooner.

3.43 When applicable, the Contractor will provide access for project Personnel and other applicable Personnel using the concept of least privileged access, meaning individuals are only granted access to those resources and systems that are required to perform their role.

3.44 The Contractor shall logically separate access between environments (e.g., development, testing, and production) so that an individual can be granted access to one environment without being able to access others.

3.45 With regards to the Contractor applications, the Contractor shall provide each individual accessing a system or application with a unique user ID and password and will prohibit user IDs and passwords from being shared.

3.46 The Customer will implement similar controls to those listed above with respect to the Contractor's confidential information.

PASSWORD MANAGEMENT

3.47 The Contractor must apply the following password management protocols:

(a) passwords must not be transmitted in clear text on the network, an approved authentication protocol must be used;

(b) if the protocol the parties agree upon uses plain text credential transmission, such as HTTP Basic authentication, LDAP simple bind or HTTP forms authentication, then any data transmission must be encrypted with an approved transport security mechanism; and

(c) initial user passwords are to be changed during the first logon, to prohibit user identifications and passwords being shared.

3.48 The Contractor will utilise the Customer's authentication standards for password expiry, account lockout threshold and external application use for any Departmental systems within the Contractor's control.

ENCRYPTION OF DATA AT REST

3.49 The Customer does not currently require encryption of data at rest for data hosted in data centres that are compliant with ISO27001:2013.

SECURITY INCIDENT REPORTING

3.50 The Contractor maintains a Security Incident monitoring, reporting, investigation, and escalation process. Contractor Personnel are required to report actual or suspected Security Incidents to a 24-hour central hotline. Once reported, Security Incidents are reviewed and escalated to appropriate teams for further investigation and analysis.

3.51 The Contractor maintains its own computer forensics, corporate investigations, and legal data privacy teams, but will also engage outside experts in these areas as needed. Where Customer Data has been affected by a Security Incident, the Contractor's data privacy legal team advises on notification or other applicable requirements. These teams work as needed with team members available to engage

on new investigations around the clock. If a Security Incident is identified as having resulted in a security breach, affected business teams work to communicate the incident promptly to the Customer and coordinate further investigative activities.

3.52 The Contractor will implement its standard processes and procedures which will be applied in the event of a Security Incident. These processes and procedures will address the relevant security incident in an efficient and timely manner and Contractor will follow these processes and procedures as soon as it is aware that a security incident has occurred (or is about to occur).

HOSTING PROVIDER

3.53 The Contractor is the Hosting Provider and will ensure any third parties used by the Contractor will adhere to substantially similar security protocols as Contractor.

4. Infor Workforce Management System as a Service Technical Security

IDENTITY AND ACCESS MANAGEMENT

4.1 The Customer's identity and access management system will be used for accessing the Infor Workforce Management System as a Service solution. The Customer will implement a federated identity solution which will interface to the Infor Workforce Management as a Service solution.

4.2 Standard features of the Infor Workforce Management System as a Service solution will be implemented to control access through defined roles and permissions.

INFRASTRUCTURE SECURITY

4.3 Infrastructure security features deployed within the environment are to be as follows:

(a) network perimeter security management via firewall appliances;

(b) network perimeter intrusion detection / prevention management by firewall appliance software modules;

(c) SSL encryption with decryption offloading provided by load balancer appliances in each site;

(d) network level segregation where communications between tiers of operating systems will be protected by firewalls; and

(e) Security Incident and event management for firewall and IDS / IPS events.

INTRUSION DETECTION

4.4 The Infor Workforce Management System as a Service solution includes intrusion detection that monitors unauthorised access attempts, breaches or suspicious activity and unexpected behaviour. The Contractor will inform the Customer of any significant alerts that may constitute a Security Incident.

4.5 The Contractor will conduct penetration testing at least annually.

NETWORK SECURITY

4.6 The Contractor will interconnect with the designated Amazon Web Services (AWS) Customer Virtual Private Cloud (VPC) network. The Customer will access the Infor Workforce Management System as a Service solution using own network infrastructure and internet service provider to connect to the VPC network.

4.7 The Customer must provide their own network connectivity (to the designated Amazon Web Services (AWS) Customer Virtual Private Cloud (VPC) network) as a low latency network and redundant with active-passive design.

4.8 The Customer will be responsible for configuration of all the required network devices (switching/routing/security) and associated security settings up to Infor Workforce Management as a Service point of presence.

4.9 The Customer will be responsible for monitoring and management of network devices at their premises.

APPLICATION SECURITY

4.10 Standard Operating Environment:
Hardened standard operating environments are created and maintained by the Contractor. This comprises the removal of unnecessary software and functionality, the disablement of unused accounts, changing default passwords for all required accounts, the configuration of access control, the installation of anti-virus software for any windows operating systems and the timely application of critical security related updates and patches.

4.11 Controlling Outbound Connections:
Required for both patching and support purposes. The Contractor will ensure that these connections are only enabled by the Contractor on an as-needed basis, and controlled by the agreed change management process.

4.12 Protection of Web Servers:
The Contractor will ensure that web servers are hardened through disabling unnecessary functionalities, and patched in a timely manner. Additionally, web servers are protected by a reverse proxy.

4.13 Application security:
The Contractor will ensure that all applications required in the Infor Workforce management as a Service solution are appropriately hardened and patched periodically as required in a timely manner.

DATA SEGREGATION IN CLOUD SOLUTION

4.14 The Contractor must ensure that comprehensive security controls are included in its cloud offering to ensure that none of the Customer Data is accessible by another of the cloud users and that the Customer's use of the Infor Workforce Management as a Service solution is not adversely affected by another cloud user. The Infor Workforce Management as a Service solution should include the following security controls to manage access to data, namely authorisation roles and data restrictions.

(a) Authorisation roles that define the transactions users are allowed to access.

(b) Data restriction that refers to the access control applied based on organisational structure.

4.15 The combination of the authorisation roles and data restriction permits a given user to only have access to transactions and data relevant to their job and to a specific Customer.

DBA AND OS ACCESS

4.16 The DBAs will not have direct access to servers such as Telnet, SSH or RDP, but will perform administrative tasks using standard tools and application access. DBA access will be restricted and internally audited regularly to ensure that unnecessary authorisations are not assigned.

4.17 The Contractor will ensure appropriate tools and processes are in place to allow a controlled access for restricted activities and emergency purposes (eg off shore access to provide 24x7 support) with audit logging functionality.

4.18 The Contractor will ensure that the host password is stored in a secure password application.

USER AUTHENTICATION

4.19 The Contractor will ensure that users authenticate to the Infor Workforce Management System as a Service solution with username and password. The Infor Workforce Management System as a Service solution frontend is a website, which is integrated with a Customer user directory. User credentials, which Customer will maintain, shall include:

(a) password complexity: minimum password length of 9 characters, must include upper and lower cases letters and must include a minimum of one number;

(b) account lifecycle: users are required to change their password once every 90 days, inactive accounts are marked as inactive and locked after 90 days, and deleted after 180 days; and

(c) account lockout: user accounts are locked after 5 failed logon attempts.

4.20 The Contractor will ensure that the Infor frontend performs:

(a) session management: with a the maximum session time of 2 hours, after which the user needs to re-authenticate to establish a new session - a user may open multiple sessions; and

(b) logon banner display: users must acknowledge the displayed logon banner setting out the security responsibilities, terms and conditions of accessing the system.

4.21 The Contractor will ensure that application single sign-on is achieved through federation services.

GOVERNANCE RISK AND COMPLIANCE

4.22 Governance, risk and compliance access control and process \control will be implemented by the Contractor to enable the following:

(a) monitoring, audit and analysis of user access; and

(b) limitations on access, with access only being granted as required to production environment data for Contractor's support staff.

Attachment 3-6 - Request Handling for High Priority Additional Service Requests and Incidents

1. Approach

1.1 In order to provide predictability in the management of Service Requests accelerated delivery for high priority Service Requests and Incident resolution in critical circumstances, the parties agree a mechanism for:

(a) dealing with Service Requests such that the work gets completed within an agreed timeframe and without causing unnecessary delays; and

(b) increasing the priority of relevant Service Requests and Incidents.

2. Initial Process

2.1 The Customer may raise a Service Request or Incident in accordance with Attachment 3-4 (Support Services).

2.2 Within two Business Days of receiving a Service Request tagged as high priority, the Contactor will provide the Customer with a time estimate to deliver a high level analysis to provide Customer with:

(a) a detailed estimate of time and cost to complete the Service Request (together with a target date for completion)

(b) within an expected three Business Days (and in any event within a maximum of five Business Days) or as agreed of the Customer's approval of the estimate, the Contractor must commence work on the Service Request.

3. Governance

3.1 During the Management Committees detailed in Attachment 3-2 (Management Committees):

(a) Service Requests will be reviewed where necessary to determine the priority for the Contractor to undertake such work; and

(b) delivery of the Service Request will be assessed against the agreed delivery timeframe target.

3.2 This Attachment 3-6 (Request Handling for High Priority Additional Service Requests and Incidents) will be reviewed on a quarterly basis in the Service Management Committee.

4. High Priority Service Requests and Incidents

4.1 Customer's Level 1 Help Desk may tag Incidents and Service Requests as high priority (**High priority Request**). The high priority tag for a High Priority Request will be carried into the Contractor's ticketing system.

4.2 Where an Incident is a High Priority Request:

(a) in the case of Severity 4 Incidents, the Incident will have its Severity increased to Severity 3 and will be moved to the top of the Severity 3 queue; and

(b) in the case of all other Incidents, the Incident will be moved to the top of the queue for the relevant Severity level.

4.3 The Contractor will track High Priority Requests with a view to ensuring that they are dealt with as promptly as possible and in the case of Incidents, within their existing Severity allocations.

4.4 Where resourcing for a High Priority Request is limited because of a higher Severity Incident or current conflict of resource time, the Contractor will agree with the Customer the re-prioritisation of other activities that should take place.

4.5 In order to prioritise a High Priority Request, the Customer may approve the Contractor to temporarily de-prioritise designated work. In such a case the Contractor will pause the Incident or Additional Service Request resolution timer by changing the ticket to a 'Pending Customer' status.

4.6 The number of High Priority Requests raised will be reported as a monthly governance item and should not exceed 5% of logged Incidents and Service Requests.

Attachment 3.7 - Transition Out Services

1. Overview

1.1 This Attachment on Transition Out Services is intended to provide for an orderly transition of the Customer from the Infor Workforce Management System as a Service solution to any of the following:

(a) an on-premise hosted and managed environment;

(b) a 3rd party hosted environment, or

(c) an alternative replacement service.

1.2 Transitioning may be required by the Customer as a result of:

(a) the Customer not being satisfied with the Infor Workforce Management System as a Service solution provision although the Customer may wish to continue to use the subscription software and all related modules;

(b) the Contractor withdrawing the Infor Workforce Management System as a Service solution whilst continuing to provide the subscription software and related modules;

(c) expiry of the Agreement at the end of the Contract Period; or

(d) the Customer's termination of the Customer Contract for cause or convenience.

1.3 To avoid doubt this section applies notwithstanding anything to the contrary within clauses 2.4 or 25.3 of the Customer Contract.

2. General Transition Out Obligations

In the event that the Transition Out Service provision is enacted, the following requisites will apply:

2.1 both parties will work together to ensure an orderly transition of the Customer off the Infor Workforce Management System as a Service solution irrespective of the reason for theTransition Out.

2.2 the Contractor must not do anything knowingly which directly or indirectly avoids, or materially prejudices or frustrates the Transition Out Services;

2.3 if Transition Out occurs, the Customer will be required to re-license software required from the Contractor under a separate Software Licensing Agreement;

2.4 the Contractor must discuss resourcing needs for Transition Out with the Customer, and must, wherever possible, use existing resources allocated to the Infor Workforce Management System as a Service solution services to provide the Transition Out Services, thereby reducing or eliminating the need to pay for additional Transition Out Services in accordance with the rates as defined by the Rate Card included in section 13 of the Schedule 12 (PIPP);

2.5 the Customer will be required to engage the Contractor for a fee, as detailed in the Rate Card included in section 13 of the Schedule 12 (PIPP), for any additional resources required to complete the transition of the service and software to the Customer's preferred target deployment environment as per section 1.1 (a) or (b) above;

2.6 The Customer will be required to engage the Contractor for a fee, as detailed in the Rate Card included in section 13 of the Schedule 12 (PIPP), to complete extract and transfer or archive the Customer Data to the Customer's preferred target environment as per section 1.1 (c) above.

2.7 The Contractor must on request from the Customer, as part of the Transition Out Services, provide a plan setting out any proposed changes to the on-going Services during execution of any Transition Out Services.

2.8 To the extent reasonably requested by the Customer, the Contractor's obligations will include (but not be limited to):

(a) co-operating with the Customer and any new contractor to ensure that there is a smooth and orderly transition to new contractor with no disruption to the Customer;

(b) providing reasonable access for the Customer or the Customer's 3rd party provider(s) to the Contractor's material kept by or on behalf of the Customer in connection with the Infor Workforce Management System as a Service and this Customer Contract;

(c) doing all such other things as the Customer may reasonably require to facilitate the successful Transition Out process.

3. Re-licensing the Software

Should the Transition Out occur for reasons outlined in sections 1.1 (a) and (b) above the following will apply:

3.1 the Customer will be required to acquire, under a separate Software License Agreement based on the then current version of Procure IT, the appropriate or equivalent number of software licenses and annual maintenance fees for the software. Pricing for such licences are listed in section 3.4 (a) and the Contractors agrees to offer the Customer these prices on this basis;

3.2 the re-licenced software licence listed in section 3.4 (a) does not include implementation, hosting, updates or maintenance of the technical environments. The assumption accompanying this is that the solution is for the Customer's internal business purposes only;

3.3 Transitioning Out of the Infor Workforce Management System as a Service will also mean transitioning out of the IVR interface; and

3.4 the Customer will not receive a refund on subscription fees paid to the point of Transition Out, however, the Contractor shall apply a credit to future additional licenses, should they be required by the Customer, reflecting a partnership approach and based on the Infor Workforce Management System as a Service solution fees paid to-date. For clarity, the impact of this credit allowance to the purchase of perpetual licenses has been applied and is listed below.

(a) If the Customer moves from Infor Workforce Management System as a Service solution to perpetual licensing, the following fees for an equivalent number of user licences will apply:

(b) Additional licences can be purchased by the Customer as needed.

(c) Modules included in the Transition Out perpetual licensing solution include licences as included in the following list and any subsequent licences acquired during the term of the Contract:

Perpetual Users being Purchased	Perpetual SKU	Perpetual SKU description	Perpetual User Type	Perpetual Support Level **

[redacted]				
[redacted]				
[redacted]				
[redacted]				
[redacted]				
[redacted]				
[redacted]				
[redacted]				

User Type Definition:

EU – "End User": "End User" means Licensee's current (i.e. non-terminated) full-time, part-time, or seasonal employees, consultants or contractors who either (i) use the Component System directly or (ii) whose records, schedules, or related data are processed by the Component System.

NU- "Named User": Allows access to the Component System up to the stated maximum number of individual named users, irrespective as to whether any such user is actively logged on to the Component Systems at a given point in time; The Licensee agrees to assign to each Named User a unique identification profile, it being agreed that to the extent Licensee uses generic user profiles as a means to access the Component System, each separate log-on accessing the Component System will be counted as a separate user.

ET- "Enterprise": Licensee and any legal entity (such as a corporation) that is majority owned or majority controlled, directly or indirectly, by Licensee. Allows unlimited use of the Component System within the licensed Business Entity.

Initial Term of Maintenance and Support is mandatory for the initial 12 month period of perpetual license purchase. This support will be offered at Infor's then current support rates. Maintenance and Support is optional after the initial 12 month period.

Support Level: Infor Xtreme ("XT") Support unless otherwise indicated.

Descriptions of the Support levels can be found at
http://www.infor.com/content/brochures/inforxtremesupportplanfeatures.pdf/
If Applicable, "XTE"= Infor Xtreme Elite (24x7)
Annual Escalation Percentage Cap for Perpetual Licenses: 4% or the then-current Consumer Price Index, whichever is greater.

Custom Code Support is required for all items (customisations) developed during the project that are not part of the core WFM product (eg. Interfaces, Cyclic Rostering, IVR Interface etc). Custom Code Support is charged as 20% of the total cost associated with Design, Build and Testing of the customisations and is charged annually in advance.

4. Transition Out Requirements

4.1 The Customer will confirm its intention to Transition Out in line with reasons as per section 1.1 above and in line with the notice periods defined in the table in Section 9.

4.2 The Contractor's consulting service group ie Infor Consulting Services (ICS) will be engaged by the Customer, to scope the work required and identify additional resourcing requirements noting requirements in sections 2.4, 2.5 and 2.6 above.

4.3 The Contractor's Consulting Service group ie Infor Consulting Services (ICS) will complete, for a fee based on pricing specified as per the Rate Card included in section 13 of the Schedule 12 (PIPP), a Transition Out plan and a quotation for the additional services to be provided to ensure a smooth Transition Out of services to the new target environment as selected by the Customer, which conforms to the specifications for the Infor Workforce Management System software. The Infor Workforce Management System as a Service solution environment will continue to be operational for the agreed duration of the Transition Out project and until the Customer confirms agreement to its cessation.

4.4 The Transition Out plan must specify the Contractor's estimate of the period of time likely to be required to Transition Out and include detail on:

(a) the technical requirements needed for successful implementation of the Infor Workforce Management System on an alternative environment.

(b) all required activities by all parties (ie Contractor, Customer and any 3rd Parties associated with the task), to enable appropriate allocation of all tasks to ensure successful transitioning;

(c) documentation, materials, records and other information required for implementation and management of the Infor Workforce Management System;

(d) information required to export Customer Data to the targeted environment;

4.5 The Contractor must ensure continuity of the Infor Workforce Management System as per the Transition Out plan until the Customer advises that the Service should cease.

4.6 The Contractor must address any other matters related to the Infor Workforce Management System as a Service solution that the Customer reasonably requires to be addressed until the Transition Out process has been completed.

5. Transition Activities:

5.1 The following is a summary of typical (but not limited to) Transition Out activities that will be covered in detail in the Transition Out plan as required in Section 4 above.

(a) the Contractor will scope and estimate the effort and resources required to undertake all Transition Out work required and present the Customer with a Variation to the contract accordingly;

(b) acceptance of the Statement of Work by the Customer is a pre-requisite for the transition scope of work, which will include a project plan and schedule, to be executed;

(c) the Customer will receive a copy of the Customer's associated data from the WFM as a Service solution;

(d) the Contractor will deploy the Customer's solution into a DEV/TEST environment based upon the current licensing available;

(e) the Contractor will perform regression testing of the re-deployed environment to confirm successful re-deployment. The scope of the regression testing will be agreed as part of the Transition Out planning stage;

(f) the Contractor will advise the Customer of any issues arising from section 5.1 (e) above;

(g) the Customer will undertake full System Integration and User Acceptance Testing (UAT);

(h) dependent on the results of section 5.1 (g) above, one or more dress rehearsals for cutover to Production may be required;

(i) the Contractor will provide User Acceptance Testing (UAT) support to the Customer staff as defined in the agreed Variation;

(j) upon receiving advice that UAT has been accepted by the Customer (and any dress rehearsals have been successfully completed), the Contractor will perform a final migration to the new PROD environment or alternative database as required by the Customer;

(k) following successful commissioning of the new environment, and following specific approval of the Customer, the Infor Workforce Management System as a Service environment will be de-commissioned. Customer Data can be, upon request, returned to the Customer so that the Customer can comply with Customer's Data Retention and Archiving policy;

(l) the Contractor will provide go-live support for a period as specifically agreed in the approved Variation; and

(m) the Contractor will provide any additional system training that the Customer deems necessary as per the agreed variation.