The Highland Council ICT Transition Programme

Data Centre Managed Service

Schedule 2.2a – Service Levels

ANNEX 1: KEY PERFORMANCE INDICATIORS

Part 1 – Key Performance Indicators Table

Table 1 – Key Performance Indicators

No.	Key Performance Indicator Title	Definition	Weighting	Service Points				
				0	1	2	3	5
				Severity Levels				
				Target Performance Level	Minor KPI Failure	Serious KPI Failure	Severe KPI Failure	KPI Service Threshold
KPI01	Severity 1 Incident resolution	Achieve full fix or effective workaround within four (4) Hours where n = the number of Severity 1 Incidents	5	n		n-1		n-2 or greater
KPI02	Severity 2 Incident resolution	Achieve full fix or effective workaround within eight (8) working hours where n = the number of Severity 2 Incidents	4	n		n-1		n-2 or greater
KPI03	Severity 3 Incident resolution	Achieve full fix or effective workaround within sixteen (16) working hours	1	95%	90%	85%	80%	79.9% or lower
KPI04	Severity 4 Incident resolution	Achieve full fix or effective workaround within twentyfour (24) working hours	1	95%	90%	85%	80%	79.9% or lower
KPI05	Number of Severity 1 Incidents	The number of Severity 1 Incidents on a rolling 3 month basis	3	3	5	7	9	10 or greater

KPI06	Wintel Server software release	Volume of server system OS software that are NOT within two releases of the current version of that system software (excluding any components of server software that the Authority has agreed in writing is not applicable)	4	0	5	10	15	16 or greater
KPI07	Wintel Database system software release	Volume of database system software that are NOT within two releases of the current version of that database system software (excluding any components of system software that the Authority has agreed in writing is not applicable)	4	0	1	2	3	4 or greater
KPI08	Infrastructure availability	Percentage availability for systems as defined in Annex. 1 Part 3 of this Schedule 2.2 (Performance Levels)	5	99.9%	99.8%	99.7%	99.6%	Below 99.6%
KPI09	Server Patching	Volume of network connected, and accessible server operating systems NOT patched against the OS vendor recommendation within 1 month	4	0	1	2	3	4 or greater

KPI10	System Backups	Number of days in the month where 100% successful backup has NOT been completed against the backup schedule with 24 hours	4	0	1	2	3	4 or greater
KPI11	Core Infrastructure software	Infrastructure components (as defined in part 2) NOT operating vendors recommended	5	0	1	2	3	4 or greater
		supported software release version within 1 month.						
KPI12	Catalogue Implementation including IMACs	Percentage achievement of standard Catalogue items within documented timescale (as set out in Annex Parts 5 & 6).	3	95%	92.5%	90%	87.5%	Lower than 87.5%
KPI13	IMAC Request – Impact Assessment	Percentage of IMAC Impact Assessments assessed by the Supplier and returned to the Authority for approval within three (3) Working Days.	3	95%	90%	85%	80%	Lower than 80%
KPI14	Asset register accuracy	Volume of CI's with incorrect attributes identified by The Authority through the audit of CMDB as defined in Part 2.	4	0	5	10	15	16 or greater

KPI15	Vulnerability scans, health checks and penetration testing	Volume of High/Critical outcomes unresolved from vulnerability scans, health checks and penetration tests conducted	5	0	1	2	3	4 or greater

Interim Performance indicators

In accordance with clause 7.1.1, the Supplier shall provide the Operational Services in such a manner so as to meet or exceed the Target Performance Level for each Performance Indicator from the relevant Operational Services Commencement Date. The Authority may agree to vary the Target Performance Levels on an interim basis where the Parties agree in the Detailed Implementation Plan to provide for phased introduction of the Services and the Authority considers that an adjustment to the Target Performance Levels would be appropriate to reflect inter-dependencies between Services. Any such interim variation of the Performance Indicators will be agreed by the Parties in writing.

Part 2: KPI Definitions 1. Availability

1.1 The IT Environment and/or the Services shall be Available (and **"Available"** shall be interpreted accordingly) when:

1.1.1 End Users are able to access and utilise all the functions of the Supplier System and/or the Services; and

1.1.2 the Supplier System is able to process the Authority Data and to provide any required reports within the timescales set out in the Services Description (as measured on a 24 × 7 basis); and

1.1.3 all Performance Indicators other than Availability are above the KPI Service Threshold.

1.2 Availability shall be measured as a percentage of the total time in a Service Period, in accordance with the following formula:

Service Availability % =

where:
MP = total number of minutes, excluding Permitted Maintenance, within the relevant Service Period; and
SD = total number of minutes of Service Downtime, excluding Permitted Maintenance, in the relevant Service Period.

1.3 When calculating Availability in accordance with this paragraph 1:

1.3.1 Service Downtime arising due to Permitted Maintenance that is carried out by the Supplier in accordance with clause 9.4 (*Maintenance*) shall be subtracted from the total number of hours in the relevant Service Period; and

1.3.2 Service Points shall accrue if:

1.3.2.1 any Service Downtime occurs as a result of Emergency Maintenance undertaken by the Supplier; or

1.3.2.2 where maintenance undertaken by the Supplier exceeds 4 hours in any Service Period.

1.4 Infrastructure Availability shall be measured in accordance with paragraph 7.

2. Response Times

2.1 The **"System Response Time"** is the round trip time taken to process a message or request of the IT Environment and/or the Services, and shall be measured from the moment the last packet of data which relates to a particular message is received at the external interface of the IT Environment until a response is generated and the first block of data leaves the external interface (including, for the avoidance of doubt, the time taken for any necessary processing).

2.2 The Supplier System Response Time shall be the average System Response Time measured over the course of a Service Period.

4. Fix Times

4.1 The **"Fix Time"** of a Service Incident is the period from the earlier time that (i) the Service Incident has been reported to the Supplier or (ii) where it has not been reported because of a Supplier failure, then the time at which the Service failure occurred, to the point of its Resolution and **"Resolution"** means in relation to a Service Incident either:

4.1.1 the root cause of the Service Incident has been removed and the Services are being provided in accordance with the Services Description and Service Levels; or

4.1.2 the Authority has been provided with a workaround in relation to the Service Incident deemed acceptable by the Authority.

4.2 Fix Times for Severity 2 Service Incidents, Severity 3 Service Incidents and Severity 4 Service Incidents shall be measured in Operational Hours.

Worked example: if the Operational Hours for a fault are 08:00-18:00, then the clock stops measuring Fix Time at 18:00 in the evening and restarts at 08:00 the following day).

4.3 Fix times for Severity 1 Service Incidents shall be measured 24 × 7.

4.4 The Supplier shall measure Fix Times as part of its service management responsibilities and report periodically to the Authority on Fix Times as part of the Performance Monitoring Report.

4.5 For the purposes of this paragraph 4, the following expressions shall have the meanings set below:

"Severity 1 Incident" means a Incident which, in the reasonable opinion of the Authority:

a) constitutes a loss of the Service which prevents a large group of End Users from working;
b) has a critical impact on the activities of the Authority;
c) causes significant financial loss and/or disruption to the Authority; or
d) results in any material loss or corruption of Authority Data;

Non-exhaustive examples:

i. a loss of power to a data centre causing failure of Services;
ii. a loss of ICT facilities in a school at an exam time; iii. a loss of access to Authority email services;
iv. a loss of key systems at critical times, for example the election system in the period leading up to an election or financial systems in the lead up to financial year end; or
v. a failure of the Services to provide user authentication service;

"Severity 2 Service Incident" means a Service Incident which, in the reasonable opinion of the Authority has the potential to:

a) have a major (but not critical) adverse impact on the activities of the Authority and no workaround acceptable to the Authority is available;
b) have a major (but not critical) adverse impact on the activities of the Authority and no workaround acceptable to the Authority is available; or
c) cause a financial loss and/or disruption to the Authority which is more than trivial but less severe than the significant financial loss described in the definition of a Severity 1 Service Incident;
d)

Non-exhaustive examples:

i. corruption of organisational database tables;
ii. degradation of performance of infrastructure components; or
iii. loss of ability to update and/or access Authority Data;

"Severity 3 Service Incident" means a Service Incident which, in the reasonable opinion of the Authority has the potential to:

a) have a major adverse impact on the activities of the Authority which can be reduced to a moderate adverse impact with the availability of a workaround acceptable to the Authority; or
b) have a moderate adverse impact on the activities of the Authority;

Non-exhaustive example:

i. inability to access data for a class of End Users;
ii. A fault that is not Corporate or Curriculum critical and affects a single user;
iii. End User's workstation or software services are unavailable to perform critical work for single End User; and
iv. A fault that is not Corporate or Curriculum critical but affects a single department or group of End Users where there is no workaround available

"Severity 4 Service Incident" means a Service Incident which, in the reasonable opinion of the Authority has the potential to have a minor adverse impact on the provision of the Services to End Users;

Non-exhaustive example:

i. inability to access data for a single customer. ii. The Service Incident has not impacted normal service and the End User can function as normal. For example an End User who has a variation to their screen resolution / image or an End User has lost their shortcut for access to an Application but a workaround is available.

5. Stop the Clock

5.1 Where an Incident requires the input of the Suppliers resolver group, the clock shall start measuring the Fix Time for the exact time period during which the rectification of the Incident is the sole responsibility of such Supplier resolver group until the incident has been resolved. For the avoidance of doubt, the clock shall only stop measuring the Fix Time at the point at which the Supplier engages the Authority internal resolver group.

5.1.1 Where the Supplier requires further information from the Authority to progress the incident and the Authority representative is not available resulting in the incident not being able to progress, the ticket will be passed back to the Authority resolver group and the clock will stop;

5.1.2 Where the Supplier 'resolves' an incident, the ticket will be passed back to the Authority resolver group and the clock will stop.

5.2 Notwithstanding the foregoing provisions of this paragraph 4, the Authority shall retain overall responsibility for the management of any such Incident until it is closed. Where input from an HC Supplier is required the Authority shall be responsible for managing compliance by such HC Supplier with any service levels or key performance indicators set out in the applicable contract with such HC Supplier.

7. Infrastructure Availability

Component	Availability Definition
VDI (Virtual Desktop Infrastructure)	VDI infrastructure is Available, providing full functionality, presenting a virtual desktop and is accepting connections by End Users. e.g. VDI Servers, Citrix Netscaler
Remote Access Gateway	Remote Access Gateway is Available, providing full functionality and establishing secure external connectivity to the IT Environment. e.g. VPN firewall, AoVPN servers
SAN (Storage Area Network)	SAN is Available, providing full functionality and servicing data read/write requests. e.g. ScaleIO
Perimeter Services	Datacentre DMZ, Network Access proxy, firewall Services are available providing full functionality and supporting requests via in scope servers and establishing internal/external connectivity to the IT Environment and WAN services where required. e.g. Perimeter firewall, internal firewall
Authentication Services	Active Directory is Available, providing full functionality and mapping the agreed permissions to End Users. e.g. Domain controllers, NAC Aruba ClearPass
Web filtering Services	Web filtering Services are available providing full functionality supporting web filtering servers. e.g. Proxy, Proxy log collector
Certificate Services	Certificate Services are available providing full functionality and supporting requests via certificate servers. e.g. PKI infrastructure
Data Centre Network	Available providing full functionality of Network within Data centre connected systems. e.g. Cisco ACI, Radware Load Balancer
SIEM Infrastructure	Providing full functionality of the Security Information and Event Management platform. e.g. QRadar
Key Line of Business Application servers	Available and providing full functionality at an OS level. Servers for applications to be defined in Part 3

Availability shall be measured as a percentage of the total time in a Service Period, in accordance with the following formula:

$$\text{Infrastructure Availability \%} = \frac{(MP - SD) \times 100}{MP}$$

where:

MP = total number of minutes within the Operational Hours, excluding Permitted Maintenance, within the relevant Service Period for all the above components; and

SD = total number of minutes of Service Downtime, excluding Permitted Maintenance, in the relevant Service Period for all the above components.

For the avoidance of doubt when calculating Infrastructure Availability in accordance with this Part II:

- Service Downtime arising due to Permitted Maintenance that is carried out by the Supplier in accordance with clause 9.4 (Maintenance) shall be subtracted from the total number of hours in the relevant Service Period; and
- Service Points shall accrue if:
  - any Service Downtime occurs as a result of Emergency Maintenance undertaken by the Supplier; or
  - where maintenance undertaken by the Supplier exceeds ***4 hours*** in any Service Period.

9. Catalogue Services

The following activities and related target performance levels are composite to the Catalogue Services KPI:

No.	Activity	Target Performance Level
KPI-12.1	Authentication Services request, e.g. enabling / denying / changes User or device access	4 working hours
KPI-12.2	Perimeter Services request, e.g. Firewall change	1 Working Day
KPI-12.3	Web Filtering Services request , e.g. proxy requests	4 working hours
KPI-12.4	Infrastructure component requests	5 Working Days
	i.e. Any update / upgrade required to maintain vendor support or to maintain capacity or availability for any infrastructure component or service, and / or Authority application (nonhardware)	
KPI-12.5	Backup and Recovery request e.g. Fulfilment of file/data recovery process (not off-site)	1 Working Day
KPI-12.6	Remote Access Gateway request e.g. Amendment of existing remote access / VPN	1 Working Day
KPI-12.7	Certificate Services request e.g. Deploy / renew / remove Certificates	1 Working Day
KPI-12.8	Any PSN Remediation activity (as per all KPI's above)	n/a

Achievement of the aggregated Catalogue Services KPI (KPI-12) is expressed as a percentage and calculated as follows:

$$\frac{\text{Sum of the number of failed requests for KPI-12.1 to KPI-12.5 inclusive}}{\text{Total number of requests made for KPI-12.1 to KPI-12.5 inclusive}} \times 100$$

10. IMACs

The following activities and related target performance levels are composite to the IMACs Service Performance KPI (see Schedule 2.1a (Services Description) for a definition of an IMAC):

No.	Activity	Target Performance Level
KPI-12.A	Any activity that does not fall within in the scope of Catalogue Service or Contract Change will be an IMAC. e.g. Implementation of new servers and/or software to accommodate a new application or service, decommissioning of IT equipment, any installation of new hardware not being replaced under an Incident, fulfilment of file data recovery not as part of an Incident, extended support hours.	As per delivery date agreed on quote.

Achievement of the aggregated IMAC KPI is expressed as a percentage and calculated as follows:

$$\frac{\text{Sum of the number of failed requests for KPI-12.A to KPI-12.I inclusive}}{\text{number of requests made for KPI-12.A to KPI-12.I inclusive}} \times 100 \text{ Total}$$

13. Vulnerability Scans

Vulnerability scans will be performed on 100% of the Data Centre infrastructure, quarterly, for the purposes of KPI 15.

Any identified High or Critical vulnerabilities will have until the end of the quarter the scan was performed in to resolve the vulnerabilities before the Target Performance Levels are measured. Should target not be met in the initial quarter, the outstanding unresolved vulnerabilities will continue to be measured and scored in accordance with KPI 15 Target thresholds each month until resolved.

Example 1: April identifies 1 Critical and 2 High vulnerabilities. If all of these are resolved by the end of June, target has been met and the score is 0.

Example 2: April identifies 1 Critical and 2 High vulnerabilities. If two of these are resolved by the month of June, this would leave 1 unresolved which would be a Minor KPI failure with a score of 5.

Example 2.1: In July the 1 remaining unresolved vulnerability is resolved, the July score will be 0;

Example 2.2: If the 1 vulnerability remains unresolved in July, this would be a Minor KPI failure with a score of 5; and will continue each month until resolved;

For the avoidance of doubt, in the above example should further vulnerabilities be identified in the July scan, they would be measured from October and added to any outstanding unresolved from April

14. Asset Register Accuracy

14.1 All Configuration Items (CIs) within the Data Centre Managed scope will be checked for accuracy against the following attributes (where applicable):

- CI Name;
- Model;
- Serial Number
- Class / sub-category;
- Description;
- Status / Operational Status;
- OS Version / Software Version;
- CPU speed/type (including cores);
- CPU count/thread;
- RAM;

14.2 Where a CI has 1 or more attributes that are incorrect, then this will count towards a single failure for the purpose of calculation of KPI 14.

14.3 Where a CI within the Data Centre Managed scope is not in the CMDB, this will count towards a single failure for the purpose of calculation of KPI 14.

14.4 The measure will include all infrastructure components detailed in Part 4 together with all physical and virtual server infrastructure.

Part 3: Key Line of Business Server Infrastructure

Wipro will provide updated list of Key Line of Business Server Infrastructure by 31 May 2021

Key Line of Business Server Infrastructure

Part 4: Core Infrastructure Software components

Wipro will provide updated list of core infrastructure components by 31 May 2021

Core Infrastructure Software.xlsx