<<insert data centre name>>

Memorandum of Agreement
for
«Organisation»

Introduction

This Agreement is entered into on DD/MM/YYYY by:

1) <<guest Organisation>>(the “CUSTOMER"); and
2) <<hosting organisation>> (the “AUTHORITY")

The Agreement is intended to set out the framework for the provision of Information and Communications Technology Services provided by the AUTHORITY.

This Agreement will be effective from the date indicated above and is on-going.

The Agreement should be read in conjunction with the accompanying schedules which set out the definition of the services provided, the way they are delivered and the charges attaching to these services.

Communication

Both bodies are committed to the principle of good communication with each other, and particularly where the requirements of one organisation may have some bearing upon the responsibilities of the other. The primary aim is not to constrain the discretion of any bodies but to allow them to make representations to each other in sufficient time for these representations to be fully considered.

Both parties will use reasonable endeavours:

- to alert each other as soon as practicable to relevant developments within their areas of responsibility;
- to give appropriate consideration to the views, ideas and suggestions of the other;
- where appropriate, to establish arrangements that allow for procedures for which responsibility is shared to be drawn up, developed jointly and improved;
- comply with their respective obligations relating to compliance with article 17 of the Data Protection Directive 95/46/EC and with schedule 1 to the Data Protection Act 1998 (‘the DPA’) contained in Schedule 12 to this Agreement.

Both parties will provide single points of contact to manage the relationship together, and to provide assurance that these persons have delegated AUTHORITY as appropriate, to work together, resolving matters of concern for either party.

The points of contact are:

For the AUTHORITY: *Name:Title*
For the CUSTOMER: *Name:Title*

The two signatories of this document will be responsible for maintaining and developing the relationship between both the AUTHORITY and the CUSTOMER.

Additionally, for escalations and disputes, they will be responsible for facilitating the resolution of issues and disagreements.

Confidentiality

Each party will use best endeavours to ensure that the information it supplies is subject to appropriate safeguards in order to avoid prejudicing its interests. Both parties accept that in certain circumstances a duty of confidence may arise and will among themselves respect legal requirements of confidentiality. In particular, the parties accept:

- it is for the body providing the information to state what, if any, restrictions there should be upon its use;
- each party will treat information which it receives in accordance with the restrictions which are specified as to its use; and
- that nothing in this Agreement shall require any party to breach an obligation of confidentiality.

All information which the AUTHORITY obtains from the CUSTOMER or becomes known to the AUTHORITY in connection with this Agreement is confidential and must not be disclosed by the AUTHORITY to any third party.

The AUTHORITY undertakes to the CUSTOMER that they shall:-

- exercise care in the use of information which is acquired in the course of their duties and protect information that is held in confidence;
- not disclose information out with the AUTHORITY and shall not use or attempt to use any such information in any manner which may injure or cause loss either directly or indirectly to the CUSTOMER or may be likely to do so;
- use their best endeavours to prevent the publication or disclosure of any confidential information; and
- Do nothing to harm the goodwill of the CUSTOMER.

The restrictions contained in this clause shall extend to any and all information of a confidential or proprietary nature belonging to any third party that is in the custody or control of the CUSTOMER and that has been disclosed by such third party to the CUSTOMER under an obligation of confidence.

Such restrictions shall continue without time limit but shall cease to apply to information or knowledge which comes into the public domain otherwise than through breach of the provisions of this statement by the AUTHORITY.

All information which the AUTHORITY obtains from the CUSTOMER or becomes known to the AUTHORITY in connection with this Agreement is not “held” by the AUTHORITY for the purposes of the Freedom of Information (Scotland) Act 2002.

The terms of this Agreement prevail over all other provisions contained in Codes of Practice, Memoranda or other agreements relative to the operation of this Agreement.

Duration

The CUSTOMER agrees to take its Co-Location Hosting services for a minimum period of 1 year. Conversely, the AUTHORITY agrees to provide these services for a minimum of 1 year.

Notwithstanding the minimum duration of this Agreement, the CUSTOMER agrees to provide the AUTHORITY with a minimum of 12 months written notice to terminate the provision of any services. The AUTHORITY also undertakes to provide the CUSTOMER with a minimum of 12 months written notice in the unlikely event that services can no longer be provided.

The AUTHORITY charges will be levied initially for any part year period and thereafter for the entire duration of a financial year. If the CUSTOMER decides to withdraw from these services part way through the year they will pay the remaining support costs up until <<dd mm>>.

Shared Risk and Liability

The AUTHORITY's liability for CUSTOMER suffering a disallowance as a consequence of one of the proscribed services not being available is nil.

Schedules

Schedule 1	Co-Location Hosting Service Definition
Schedule 2	CUSTOMER's use of the Data Centre
Schedule 3	AUTHORITY management information
Schedule 4	Data protection

Entire Agreement

This Agreement (including the Schedules hereto) together with any documents listed below:

- AUTHORITY Customer Service Handbook;
- Code of Conduct;
- IT Security Policy

constitute the entire agreement and understanding between the parties relating to the provision of Co-Location Hosting service and supersede all previous agreements and understandings. In the event of any conflict or inconsistency between this

Agreement (including the Schedules hereto and the documents as listed above), the order of precedence shall be this Agreement (including the Schedules hereto) and then the documents referred to.

Signed for and on behalf of the CUSTOMER
By :
Name :
Title :
Date :
Place/town :
Witness :
Witness' full name :
Witness' address :

Signed for and on behalf of the AUTHORITY
By :
Name :
Title :
Date :
Place/town :
Witness :
Witness' full name :
Witness' address :

Schedule 1 - Co-Location Hosting Service Definition

General Description

The following sections provide a definition of the co-location service offered to «Organisation» as a customer of the AUTHORITY's Data Centre.

Standards

The AUTHORITY's Services are designed, supported and managed in accordance with the information security standard ISO / IEC 27001 and to IT Infrastructure Library (ITIL) standards. The AUTHORITY adheres to a range of standards and methodologies that ensure that full regard has been given to:

- Legal requirements
- Government Initiatives
- Published industry best practice
- Scottish Government strategies and policies (see section 6.0 to see how customers can also influence change)

Customers, therefore, can be confident that the services will be reliable, available and have the capacity to perform well. All products used to provide services have been fully tested to ensure optimum performance.

Performance of the Data Centre BEMS is continually monitored to identify actual or potential problems and ensure any adverse impact is minimised. The systems employed have been designed with sufficient capacity to meet all known user needs and with spare capacity for peaks in usage and increases in numbers of users or services. Systems are continually assessed to ensure that capacity continues to meet requirements and that future needs are considered.

The AUTHORITY is committed to the continuous development and improvement of its services. We welcome and actively seek feedback, comments and suggestions from users of the AUTHORITY Services. Periodic surveys are carried out to determine the overall level of user satisfaction with these services and the results are published.

Service Availability

The Data Centre services operate continuously and are available <insert availability e.g 365 x 24 x 7>>. The Prime Service Time is <<insert times e.g. 0800 to 1800 Monday to Friday>> to align with the normal working day, but customers can access and use Services outside these hours.

Planned / Unplanned Maintenance

A comprehensive planned preventative maintenance (PPM) regime is conducted on all DC plant and equipment which follows manufacturers' guidelines. The Tier <<insert level>> design together with the PPM regime should ensure continued availability of all critical Mechanical and Electrical components.

Planned Maintenance which requires any Service Downtime is scheduled in advance and in consultation with customers affected, to ensure that as far as possible, critical business periods are not impacted. The AUTHORITY aims to consult customers when planned downtime is being scheduled, and will try to offer alternatives or workarounds where possible.

Despite these best endeavours there may still be occasions it becomes necessary to conduct some unplanned works. The AUTHORITY therefore reserves the right to carry out any such remedial action in order to restore full service within a time frame that reflects the severity of any situation. After assessing the situation the AUTHORITY will notify customers of the work to be carried out and ensure any period of increased risk or disruption to service is minimised. The timing of any repair work will be agreed after consultation with customers.

All incidences of unscheduled service downtime are treated as Priority. The service impact of each downtime incident is recorded and reported in regular Service Delivery Reports.

Operational Support

Support Levels (referencing the AUTHORITY Service Standards)

Level 1: the AUTHORITY Help Desk

Incidents should be reported to the AUTHORITY Helpdesk (<<insert phone number>>). The Helpdesk resolves the issue at first contact, if possible, and if not logs the request and assigns the incident or change request to the appropriate second line support team.

The Helpdesk is available <<insert times e.g. 0800 – 1800>> (Prime Service Time), << insert days e.g. Monday to Friday>> and at other times by prior agreement. Outwith these hours, a voicemail service is available for messages to be recorded. These are logged into the Help Desk system at the start of the next working day. A call reference number is given and should be used for any future enquiries about the status of the call.

Level 2: Specialised support teams

Specialist support teams handle all calls referred to them via the Help Desk. They provide specialist support for different elements of the AUTHORITY Services and each team is highly experienced in its subject.

Level 3: Specialist sub-contractors

The AUTHORITY has a number of contracts in place to provide specialist support and advice on Data Centre maintenance. These contractors handle calls assigned to them using the Help Desk system.

Support Times

Support services are available during Prime Service Time.
If a service is unavailable in Prime Service Time, our performance target is:-

- initial response within 45 minutes
- full availability of service within four hours (external maintenance not required)
- by the end of the next working day (if external maintenance required).

If a service is unavailable out with Prime Service Time, our performance target is:-

- initial response next working morning
- on-site attendance next working day
- full availability by the end of the next working day

As a general rule, no support service is available out with Prime Service Time or on the public and privilege holidays shown in the table below.

Public Holidays	
Good Friday	Autumn Holiday Monday (Edinburgh)
Easter Monday	St Andrew's Day
May Day	Christmas Day
Queen's Official Birthday	Boxing Day
Spring Holiday Monday	New Year's Day
Friday(p.m.) preceding Autumn holiday	2nd January

At these times calls are recorded via the voicemail facility. These calls will be dealt with on the next business day. Local arrangements may be set up by prior agreement with the AUTHORITY.

Service targets

The AUTHORITY has target resolution times for all incidents logged on the HelpDesk System. Incidents are categorised as being either Priority 1 or Priority 2, with Priority 1 incidents taking precedence. Incidents are categorised as Priority 1 where they affect the delivery of critical systems or impact a significant number of users.

Priority Level	Target Resolution Time
1	6 Hours
2	8 Hours

the AUTHORITY measures its performance against these targets and publishes reports as part of the Management Information provided to customers.

Escalation

An automatic escalation process is used to ensure that all calls are handled in a consistent way, to ensure no calls are overlooked and to highlight any which require additional resources or expertise to resolve.

All logged calls are allocated pre-defined resolution times and escalation or notification paths. Incidents which remain Open when resolution times have ended are automatically escalated by the Helpdesk System. For priority level 2 incidents the escalation path and timetable is:

Escalation Level	After elapsed time	Escalated to
1	6 hrs (75%)	Support Team Leader
2	8 hrs (100%)	Support Manager
3	12 hrs (150%)	IT Support Manager
4	16 hrs (200%)	Chief Technical Officer

The escalation times for priority level 1 incidents use the same process but the times between each escalation level are 75% shorter.
On escalation, we review the call to ensure that the call status has been updated and the customer contacted. The resolving support team is responsible for these actions.

Call Closure

When an incident is resolved, the support team who provided the fix will contact the customer to agree closure and close the call. If it proves difficult to contact the customer, the support team will send an email, containing the call reference, notifying the customer of their intention to close the call. The support team will then close the call.

Service Feedback

On closure of Helpdesk incidents, a feedback card is issued to the user by email to seek their views on the service.

Complaints

If a customer is dissatisfied with any aspect of service they have received from the AUTHORITY, they are encouraged to contact the AUTHORITY Support. All complaints made to any member of the AUTHORITY, whether made in person, over the telephone or by email, will, however, be handled in the same way, using the AUTHORITY complaints procedure.

The details of any dissatisfaction raised will be forwarded directly to the IT Support Manager. The manager will clarify the nature of the problem and contact the customer to try to deal with the issue(s) informally.

If the customer is not satisfied with the response, they will be offered the opportunity to formally log the issue as a complaint. The customer will be provided with a reference number and expected response time.

The complaint will then receive a full investigation and a report will be sent to the Head of Data Centre & Network Services.

The customer will then be contacted by the head of customer support within 10 working days, advising the outcome of the complaint and providing a copy of the final report.

If the customer is still not satisfied, the matter will be escalated further to Chief Information Officer.

It is the AUTHORITY policy to review any complaints received on an on-going basis to ensure that lessons are learned from issues that have arisen.

Service Measurement

The objectives of the Service Levels are to:

- Ensure that the Services are of a consistently high quality and meet the requirements of the Customer;
- Provide a mechanism whereby the Customer can attain meaningful recognition of inconvenience and/or loss resulting from the AUTHORITY's failure to deliver the level of Service for which it has contracted to deliver;
- Incentivise the AUTHORITY to meet the Service Levels and to remedy any failure to meet the Service Levels expeditiously.

Service Metrics – Service Level Agreements (SLA)

The main service delivery elements below will be measurable services and form the core part of the Quarterly Performance Monitoring Report, – the production and issue of which is in itself is a service target. This report details the contracted Performance Indicators (PI) and Key Performance Indicators (KPI) to illustrate performance.

Key Performance Indicators – Summary

- Service Availability during Prime Service Time and Un-Supported Prime Service Time;
- Service Incidents - Acknowledge, Assign and Update target times;
- Service Fix Times for Service Failures;
- Customer Service User Satisfaction – Incidents and Problems – satisfaction targets;
- Change Management Performance - – Access Requests (AR); Requests for Changes (RFC);
- Electrical Failover Tests – Failover Time Objective threshold performance;

- Rack Power Usage – BEMS monitoring of power consumption on a per rack basis.

Service Metrics: Performance Indicators (PI) Detail

PI	Title	Definition	Target
PI#1	Performance Monitoring Report to the GPB Lead Contact by 10th Core Service Day of each Month	All requested Performance Monitoring Reports should be sent to the contact by the 10th Core Service Day of each month	100%
PI#2	1 Electrical Failover Test per calendar year	The purpose of electrical failover testing is to ensure that the service can continue in the event of a failure to the mains electricity supply. the AUTHORITY will provide a report, containing all tests executed, a record of the result obtained , and a record of defects raised and resolved, within 20 Core Service Days of the test	100%
PI#3	Customer Satisfaction Form sent out for all calls logged through the SG helpdesk	A Customer Satisfaction form should be sent out for all calls logged via the helpesk to cover the AUTHORITY assigned calls.	100%
PI#4	Incident Response Times:	Acknowledge and Assign: within 45 minutes if logged during Core Helpdesk Hours or if logged out with Core Helpdesk Hours within 30 minutes of the start of the next period of Core Service Helpdesk Hours. Updates :all updates to Service Desk Calls should be passed to technical domain within 15 mins	100%
PI#5	Fix Times:	the AUTHORITY shall dedicate all necessary resources on a priority basis to resolve a service failure as per the AUTHORITY published Service Levels	100%

PI#6	Requests For Change : Response required	the AUTHORITY will ensure that on receipt of completed RFCs they will respond within 10 Core Service Days with either approval or analysis and comment on the potential costs. Access Requests will be acknowledged on the date of receipt within normal working hours.	100%
PI#7	Rack Power Usage	the AUTHORITY will monitor usage to ensure that it does not exceed contracted 4kWh	100%

Service Metrics: Key Performance Indicators (KPI) Detail

KPI	Title	Definition	Target
KPI#1	Availability during Prime Service Time	Availability of the Service during Prime Service Time, Monday to Friday., 08:00 until 18.00 Local Time (Edinburgh UK) including all statutory holidays as published on www.scotland.gov.uk/publications	99.5%
KPI#2	Availability out with Prime Service Time	Availability of the Service during Unsupported Prime Service Time, all day Saturday & Sunday; Monday to Friday before 08:00 or after 18.00 Local Time (Edinburgh UK) including all statutory holidays as published on www.scotland.gov.uk/publications;	95%
KPI#3	Incident Response Times as per PI#4	Acknowledge and Assign: within 45 minutes if logged during Core Helpdesk Hours or if logged out with Core Helpdesk Hours within 45 minutes of the start of the next period of Core Service Helpdesk Hours. Updates :all updates to Service Desk	2 SLA failures per month

		Calls should be passed to technical domain within 15 mins	
KPI#4	Fix times as per PI#5	the AUTHORITY shall dedicate all necessary resources on a priority basis to resolve a service failure as per the AUTHORITY published Service Levels	2 SLA failures per month
KPI#5	Customer satisfaction	Customer satisfaction forms returned with a satisfactory marking or above	90%
KPI#6	RFC Response Time	the AUTHORITY will ensure that on receipt of completed RFCs they will respond within 10 Core Service Days with either approval or analysis and comment on the potential costs.	1 SLA failure per month
KPI#7	Power usage	«OrganisationAbbreviation» shall not exceed the agreed power usage of their installation.	99.5%

Communications with Customers

the AUTHORITY recognises the importance of open communications with Customers and utilises the following channels

Method	Intended Audience	Timing/Frequency
Telephone	«OrganisationAbbreviation» Lead Contacts	As and when required
Helpdesk 0131 244 8500	All Users	As and when required
Incident Updates	«OrganisationAbbreviation» Lead Contacts	As and when required
Access Request Form email	«OrganisationAbbreviation» Lead Contacts	24 hours prior to data hall access
Performance Report	«OrganisationAbbreviation» Lead Contacts	Prior to Service Review Meeting
Service Review Meeting	«OrganisationAbbreviation» Lead Contacts	Quarterly
Service Message	All data centre users	Prior to essential maintenance

Additional Services Provided by the AUTHORITY

The following support services can be provided to the CUSTOMER by the AUTHORITY at an additional cost (based on the published AUTHORITY Service catalogue rates) to the Co-Location Hosting service.

Tape backup services
the AUTHORITY operates a full tape library service comprising off-site storage at secure facilities. Typically, tape rotation operates on a 28 day basis. Full backups are taken each Friday, with incremental backups taken on other days.

Tapes are stored on site at <<insert location>> within fireproof safes before being despatched off site. Whilst still at << insert location>>, data can be recovered from tapes at no further cost. Once they have been taken off site there is an administration charge levied to return the tapes to site, if required in exceptional circumstances.

Hot hands
the AUTHORITY can assist the remote configuration of the CUSTOMERS systems by performing local tasks which need physical interaction with the equipment. This would be performed under the direct instruction of the «OrganisationAbbreviation» technical domain.

Co-Location Service Development

Overview

the AUTHORITY reserves the right to continue to develop and improve all its services and products in order to exploit new and advancing technology and guidance and to meet the demands of developing policies and legislation.

the AUTHORITY will work in partnership with its customers to this end so that developments to any of the services bring increased business benefits to both the AUTHORITY and its customers.

Change management relates to the processes and procedures involved in changing, adding or removing services. This section details the ways in which change will affect you, and how you can help us deliver the best possible service to your organisation.

Change can occur for a number of different reasons e.g.

- New products (software or hardware)
- New versions of existing products (e.g. new software release or new hardware model)
- Upgrades to existing products (e.g. software service release)
- Minor change to current system or service configuration (e.g. Software Patch management or more equipment)

Changes may be initiated by the customer, by the AUTHORITY or by the system owners whose systems are accessible through the Co-Location Service.

Customer-initiated Change

Customers may wish to request changes to the service.
the AUTHORITY will supply a Request for Change (RFC) form (attached at Schedule 2 section 7) to be used when requesting additions or changes. When completing an RFC, please ensure that all relevant information is provided, to prevent a delay in servicing any particular request. Where there are cost implications of the change, a proposal will be returned for financial approval prior to any work commencing.

The AUTHORITY initiated Change

The AUTHORITY reserve the right to introduce new products and services and new versions of existing ones. When we do this, we make every effort to give customers as much notice as possible and to ensure that each product is adequately tested. While we test against existing the AUTHORITY products and applications, we require customers to test their own installations to assess the risks and impacts associated with system change

Target Delivery Times for Changes

Installations, moves, additions and changes of hardware and software on the available environments are typically delivered within the following timescales:-

Activity	Typical Timescale
User Access	24 hours
New User Access	10 days

Timescales for other changes are not pre-defined. Where such changes are requested, an assessment of the change will be made and a target completion date provided to the customer.

the AUTHORITY monitors its performance at meeting these delivery targets and completion dates and produces regular reports for its customers as described in Schedule 3.

IT Service and Business Continuity

the AUTHORITY maintains a detailed IT service continuity plan, which is continuously monitored and reviewed, in a perpetual state of readiness. It is also tested on a regular basis to ensure that it is fit for purpose.

This plan covers the infrastructure provided by the AUTHORITY, including Mechanical & Electrical devices but NOT any business application servers, switches etc., managed or administered by the customer or their service provider.

Customer organisations must ensure that they have a business continuity plan for their organisation that can be invoked as appropriate. While customer organisations

ultimately own this plan, the AUTHORITY is pleased to provide business consultancy advice to develop and optimise business continuity plans where appropriate.

Schedule 2 – Data Centre Usage

Facilities Used

The CUSTOMER uses «RacksUsed» rack(s) in the AUTHORITY Data Centre. This is located in the AUTHORITY Data Centre <insert name of room>>.

The following facilities are provided.

- The CUSTOMER systems at rack positions «RackPosition» inclusive.

Set Up Charge

The setup charge for the services proposed is £X, exclusive of VAT. The cost breakdown per rack is XXXXXXX

Part No.	Server Rack & Components	Unit Price	Installation	Total	Quantity	Sub Total	Total
AR3150	APC Rack Netshelter SX 78"Hx29"Wx42"D				1		
AP8853	32Amp Metered PDU				2		
CPI 13675-001	Koldlok Brushed Floor Grommet				1		
	Floor Grille				1		
							XXXX

This charge is for the work to support the installation and preparation of the rack and rack PDUs. This includes the rack and cabling within the data centre to connect to the customer's network services as well as any out of hours attendance by the AUTHORITY personnel.

Annual Service Charge

The annual charge for locating «RacksUsed» rack(s) for a minimum period of twelve months from the date of installation is £X exclusive of VAT.

VAT will apply to the Setup and Annual Service Charges as «OrganisationAbbreviation» has a separate VAT registration from that of the Scottish Government.

The Annual Service Charge will apply from the start of the month when installation is completed and will continue, at the end of any agreement, until the CUSTOMER equipment is removed from the Data Centre.

The charge includes the provision of the electricity to power the customer's equipment and a share of the power to provide the data centre environment.

Charges will be subject to an Annual Cost Review with any change applicable from the start of the following financial year. Power costs are a significant element of the hosting charge and the AUTHORITY reserves the right to review the charge for the co-location service if the consumption of or tariff for electricity increases significantly. Any increase will be based on a simple cost recovery model.

Rack and Power

The power supply train is built to Tier 3 Standards (N+1) with all critical components being concurrently maintainable.
The power supply train on site has been duplicated to meet Tier 3 standards and its aim of eliminating any single points of failure. Each rack in the DC has two separate 32 amp power supplies, referred to as an “A” and a “B” supply, these are located below and adjacent to each rack

Each supply starts at its own high voltage transformer and is connected via switchgear and power distribution units to each rack within the Data Centre. Each supply is protected by one of two centralised uninterruptible power supply (UPS) and by one of two generators. Each generator and UPS can individually take the site load and in the event of a transformer failure operation of a bus coupler would ensure continuity of supply to all 32 amp supplies.

the AUTHORITY have standardised on the use of APC NetShelter SX racks, these are provisioned with 2 no. 32Amp Power Distribution Units. The installation and preparation of these components can be carried out by the AUTHORITY on behalf of the customer. The rack dimensions are 42u (750 x 1070) and have lockable front, rear and sides. The doors come with standard lock and key but can be fitted with individual locks and also an optional combination lock with key override.

The Data Centre is designed to host racks with a maximum power of 4 KWh. The rack PDU’s are manageable via SNMP and provide power consumption statistics. If requested the AUTHORITY can provide continual monitoring and reporting of the electrical consumption down to rack level.

The CUSTOMER rack(s) will be located in <Insert location>> at Row «Row» and will be labelled with the following rack position(s) ‘«RackPosition»’.

Network Connectivity

The provision of the external network connectivity to the Data Centre is the responsibility of the customer. the AUTHORITY will provide assistance with the installation of the required services but these services must be ordered by customer.

The AUTHORITY will provide connectivity from the Telecoms providers’ racks to the customer equipment racks, a charge to cover the cabling costs will apply and this will be included in the one off setup charge.

At present the Data Centre uses services provided by a number of Telecoms providers including <<insert providers e.g. C&WW, BT, VirginMedia and Verizon>>. Customers are free to add other providers.

Environment
Cooling system is designed and built to Tier 3 Standards (99.98% uptime), equates to 1.6 hours of site caused downtime p.a.

The operating temperature and humidity within the Data Rooms is continuously monitored via the BEMS. Currently Data Room 2 is set to operate at 25 +/- 2 degrees Celsius and 35% humidity. As part of our initiative to use energy efficiently we constantly monitor the environment and in consultation with DC customers we may make adjustments to these settings.

Very Early Smoke Detection Apparatus (VESDA) is installed in the data rooms and electrical plant rooms to provide first level detection and alerting of any risk of fire and an FM200 gas fire suppression system is installed in the data and plant rooms to prevent any fire. This system reduces the oxygen to a level at which fire is not possible. Customer's equipment racks should be kept clear of any combustible material in particular paper and cardboard as these systems are sensitive to airborne particulate matter. A dedicated build room is provided as an area to unpack and configure equipment prior to installation.

Security / Access

The facility is contained with the Scottish Government Saughton House site which benefits from multi camera surveillance and monitoring 24 hours a day. Video cameras are installed inside the Data Rooms and all doors have access controls. The DC is designed with the objective of being "a lights out" facility with access only required to install or repair IT hardware. It is anticipated that virtually all systems management activity will be completed remotely.

Access to the Data Centre is strictly controlled. Customers and their contractors will have to comply with the access rules. Baseline clearance (BPSS) is required to gain access to Scottish Government (SG) buildings and a permit to work must be approved in advance to gain access to the DC. Planned changes require 24 hours advance notice but Emergency Access can be provided with a minimum of 1 hour notice. Details of BPSS clearance are available from the AUTHORITY IT Security Branch (*insert contact details*).

Access to the Data Rooms is strictly controlled and can only be arranged by following the 'Data Room Access Procedure'. A Permit to Work will be required before any moves, adds & changes are carried out this requires the approval of the Data Centre Manager and will be provided on receipt of any necessary risk assessment and method statement.

Planned or Emergency Access to the data centre during the working week <<insert timings e.g. Mon to Fri between 07:00 and 19:00>> is included within the standard service. Access out with these times can be arranged but may incur additional

charges i.e. in the event of a member of the AUTHORITY staff being required to attend, in this case the relevant hourly rate will be charged.

Monitoring and Alerting

The DC plant is monitored continuously by a dedicated Building and Energy Management System (BEMS). The system provides over 160 different alarms and determines which combination of alarms are critical and require an immediate response. All alarms are reported to the DC plant engineer and critical alarms are monitored on a 7 X 24 hour basis by our Maintenance Contractor who provides a one hour on-site response.

Schedule 3 – Management Information

A standard quarterly report will be provided by the AUTHORITY.

The frequency of the report would be agreed between the AUTHORITY and the CUSTOMER.

Additional service information can be made available, but this would be a chargeable service, with costs dependent on the information required.

Schedule 4 data protection

1. Data Protection Background

(A) The CUSTOMER processes personal data in connection with its statutory functions under the Legal Profession and Legal Aid (Scotland) Act 2007;

(B) The AUTHORITY provides Information and Communications Technology Services to the CUSTOMER in the course of which it processes personal data on behalf the CUSTOMER;

(C) Article 17(2) of the Data Protection Directive 95/46/EC (as hereinafter defined) provides that, where processing of personal data is carried out by a processor on behalf of a data controller the controller must choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures;

(D) Articles 17(3) and 17(4) of the Data Protection Directive require that when processing is carried out by a processor on behalf of a controller such processing must be governed by a contract or legal act binding the processor to the controller stipulating, in particular, that the processor shall act only on instructions from the controller and that the technical and organisational measures required under the appropriate national law to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, shall also be incumbent on the processor;

(E) Paragraph 7 of Part I of schedule 1 to the Data Protection Act 1998 ("the seventh data protection principle") requires that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;

(F) Paragraph 12(a)(i) and (ii) and paragraph 12(b) of Part II of schedule 1 to the Data Protection Act 1998 require that where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh data protection principle unless

> (a) the processing is carried out under a contract which is made or evidenced in writing and under which the data processor is to act only on instructions from the data controller, and
> (b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh data protection principle;

(G) In compliance with the above mentioned provisions of Article 17 of the Data Protection Directive, and schedule 1 to the Data Protection Act 1998 the

CUSTOMER and the AUTHORITY wish to enter into this processing security Agreement.

The parties hereby mutually agree as follows:

In this Schedule the following words and phrases shall have the following meanings, unless inconsistent with the context or as otherwise specified:

"Data Protection Directive" means Directive 95/46/EC of the European Parliament and Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
"Data" means information which
(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
(b) is recorded with the intention that it should be processed by means of such equipment,
(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68 of the Data Protection Act 1998, or
(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d);

"National law" means the law of Scotland;
"personal data" means data which relate to a living individual who can be identified –

(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

"processing" in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –
(a) organisation, adaptation or alteration of the information or data,
(b) retrieval, consultation or use of the information or data,
(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
(d) alignment, combination, blocking, erasure or destruction of the information or data;

"relevant filing system" means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible;
"sub-contract" and **"sub-contracting"** mean the process by which either party arranges for a third party to carry out its obligations under this Agreement and the

“sub-contractor” shall mean the party to whom the obligations are sub-contracted; and

“Technical and organisational security measures” means measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of processing.

2. Consideration
In consideration of the CUSTOMER engaging the services of the AUTHORITY to process personal data on its behalf the AUTHORITY shall comply with the security, confidentiality and other obligations imposed on it under this Agreement.

3. Security Obligation of the AUTHORITY
3.1 The AUTHORITY shall only carry out those actions in respect of the personal data processed on behalf of the CUSTOMER as are expressly authorised by the CUSTOMER.
3.2 The AUTHORITY shall take such technical and organisational security measures as are required under its own national law, and in particular under the seventh data protection principle in schedule 1 to the Data Protection Act 1998, to protect personal data processed by the AUTHORITY on behalf of the CUSTOMER against unlawful forms of processing. Such technical and organisational security measures shall include, as a minimum standard of protection, compliance with the legal and practical security requirements set out in Appendix 1 of this Schedule.

4. Confidentiality
4.1 The AUTHORITY agrees that it shall process personal data under this Agreement on behalf of the CUSTOMER in confidence. In particular, the AUTHORITY agrees that, save with the prior written consent of the CUSTOMER, it shall not disclose any personal data supplied to the AUTHORITY by, for, or on behalf of, the CUSTOMER to any third party. For these purposes, “third party” means, in relation to any personal data, any party other than
(a) the data subject,
(b) the CUSTOMER, and
(c) the AUTHORITY
and, for the avoidance of doubt, excludes any part of the Scottish Government, and any person employed by or providing any service to the Scottish Government, other than the AUTHORITY.

4.2 The AUTHORITY shall not make any use of any personal data supplied to it by the CUSTOMER otherwise than as is necessary for the provision of the services to the CUSTOMER.

4.3 The obligations in clauses 4.1 and 4.2 above shall continue for a period of five years after the cessation of the provision of the services by the AUTHORITY to the CUSTOMER.

4.4 Nothing in this Agreement shall prevent either party from complying with any legal obligation imposed by a regulator or court. Both parties shall however, where

possible, discuss together the appropriate response to any request from a regulator or court for disclosure of information.

5. Sub-contracting
5.1 The AUTHORITY shall not sub-contract any of its rights or obligations under this Agreement without the prior written consent of the CUSTOMER.
5.2 Where the AUTHORITY, with the consent of the CUSTOMER, sub-contracts its obligations under this Agreement it shall do so only by way of a written agreement with the sub-contractor which imposes the same obligations in relation to the security of the processing on the Sub-contractor as are imposed on the AUTHORITY under this Agreement.

5.3 For the avoidance of doubt, where the sub-contractor fails to fulfil its obligations under any sub-processing agreement, the AUTHORITY shall remain fully liable to the CUSTOMER for the fulfilment of its obligations under this Agreement.

6. Term and Termination
6.1 This Agreement shall continue in full force and effect for so long as the AUTHORITY is processing personal data on behalf of the CUSTOMER.
6.2 Within 14 days following termination of this Agreement the AUTHORITY shall, at the direction of the CUSTOMER, (a) comply with any other agreement made between the parties concerning the return or destruction of information or data, or (b) return all information or data passed to the AUTHORITY by the CUSTOMER for processing, or (c) on receipt of written instructions from the CUSTOMER, destroy all such information or data unless prohibited from doing so by any applicable law.

Appendix 1

This is Appendix 1 referred to in Schedule 4 to the foregoing Agreement between the AUTHORITY (Information Systems and Information Services) and «OrganisationAbbreviation» («Organisation»)

1. Legal Requirements
The AUTHORITY shall, in respect of the processing of personal data on behalf of the CUSTOMER, identify and comply with any specific security provisions imposed by its national law.

2. Practical Security Measures
2.1 In compliance with its obligations under clause 3.2 of Schedule 12 to the Agreement with regard to the processing of personal data on behalf of the CUSTOMER, the AUTHORITY, as a minimum requirement, shall give due consideration to and take appropriate action in order to comply with its obligations under this Agreement and the national law in relation to the following types of security measures:

2.1.1 Information Security Management Systems;
2.1.2 Physical Security;
2.1.3 Access Control;
2.1.4 Security and Privacy Enhancing Technologies;
2.1.5 Awareness, training and security checks in relation to personnel;
2.1.6 Incident/Response Management/ Business Continuity; and
2.1.7 Audit Control/ Due Diligence.

3. Definitions and Interpretation
In this Appendix, the following words and phrases shall have the following meanings, unless inconsistent with the context or as otherwise specified:

"Information Security Management Systems" means that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security, and includes the statement of an information security policy.

"Physical Security" means the layout and design of facilities, combined with suitable security measures, such as lockable doors, alarms, security lighting or CCTV, used to prevent unauthorised access and to protect personal data, and includes the measures taken to control and monitor access to personal data. Within Scottish Government this is achieved through a combination of manned guarding and an automated access control system complimented by a photographic security pass system;

"Access Control" means procedures for authorising and authenticating users, e.g. the use of passwords, and software controls for restricting access in order to protect personal data;

“Security and Privacy Enhancing Technologies” means computer tools, applications and mechanisms such as anti-virus software, firewalls and encryption software, which – when integrated in online services or applications, or when used in conjunction with such services or applications – allow the protection of personal data processed by such applications;

“Awareness, training and security checks in relation to personnel” means the programme of making staff aware of, and providing training to staff in respect of, their legal obligations in relation to processing data, as well as the baseline security checks on personnel that are mandated within Scottish Government as part of its ongoing ISO / IEC 27001 and GSI security accreditation;

“Incident/Response Management/ Business Continuity” means the monitoring and detection of events which could breach data security requirements of this Agreement or the national law, and the execution of proper responses to those events. Business continuity is the activity performed to ensure that business critical functions will continue to be available to customers, suppliers, regulators and other entities in the event of a security event;

“Audit Control” means having in place security audit arrangements to ensure that the security procedures in place are effective, including good record keeping, auditing of who has access to personal data, logging of such access and auditing of compliance with security procedures; and

“Due Diligence” means the taking of all reasonable steps to ensure that the requirements of data security in this Agreement and in the national law are complied with.

Appendix 2

Summary of Responsibilities

AUTHORITY:

1. Provide and maintain a resilient data centre architecture
2. Test the Mechanical & Electrical systems regularly
3. Notify «OrganisationAbbreviation» of planned preventative maintenance to infrastructure in advance
4. Control access to data hall
5. Provide guidance on Health and Safety use within VESDA areas
6. Respond to service failures within SLA
7. Respond to Requests for Change within SLA
8. Chair Quarterly Service Meetings
9. Monitor and provide performance reports for Service Meetings

CUSTOMER:

1. Procure an external network supply at own cost
2. Give 24 hours' notice of intention to access the data centre in person.
3. Provide and maintain an accurate list of staff and contractors who require access to the data centre for BPSS clearance
4. Ensure only BPSS cleared contractors attend the data centre (or provide a BPSS cleared escort)
5. Familiarise themselves with and follow all Health & Safety guidance before entering VESDA areas.
6. Use build area to unbox and assemble equipment prior to installation in data centre.
7. Keep rack area clear and tidy. – No packaging is allowed in data centre
8. Do not exceed agreed power consumption of racks.
9. Attend Quarterly Service Meetings