DSB DISASTER RECOVERY AND BUSINESS CONTINUITY POLICY

1 GENERAL

1.1 This Disaster Recovery and Business Continuity Policy sets out the disaster recovery and business continuity processes that will apply to the DSB Services.

1.2 This Disaster Recovery and Business Continuity Policy forms part of the Agreement agreed between the User and the DSB. Defined terms shall have the same meaning as set out in the main terms of the Agreement and as otherwise set out herein.

1.3 Disaster recovery and business continuity are topics the DSB Technology Advisory Committee (TAC) regularly considers. Information regarding the TAC and its charter can be found on the DSB website.

2 DSB PROCESSES

2.1 The DSB Service is built and configured on the Amazon Web Services public cloud ("**AWS**") for High Availability within an AWS Region. BCP methodology will only be required in the event of a complete region failure.

2.2 The service is built with three Availability Zones ("**AZ**") present in each region. Automatic server side failovers and load balancing are present as per AWS best practice to ensure a Highly Available (HA) environment.

2.3 In the event a whole region is offline the DSB will failover to another region of which two are configured and kept updated with the relevant software patches and versions. The data is replicated in real time ensuring there are no database discrepancies between AZ to AZ and Region to Region.

2.4 Once the production environment is configured, the DSB will annually test the failover methodology between the AZ-AZ and Region-Region for service continuity.

2.5 The DSB Service has been designed to ensure that there is no single point of failure in the network design. All production servers are at least paired (i.e. there will be at least one other server doing the same job that can take on the work), replicated and backed up in real time.

2.6 The DSB Service infrastructure and network traffic are continuously monitored throughout the stack and alerts will be sent to the DSB when resources or bandwidth thresholds are breached.

2.7 Server configurations shall be backed up securely.