

DSB DR and Business Continuity Policy

I General

- I.1 This Disaster Recovery and Business Continuity Policy sets out the disaster recovery (**DR**) and business continuity processes (**BCP**) that will apply to the DSB Services.
- I.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 and as otherwise set out herein.
- I.3 Disaster recovery and business continuity are topics the DSB Technology Advisory Committee (**TAC**) regularly considers. Information regarding the [TAC](#)¹ and its [Charter](#)² can be found on the [DSB website](#)³.

2 MSP Site BCP

- 2.1 The DSB is operated by a management services partner ("**MSP**") whose staff are located at two regional sites ("**MSP Sites**").
- 2.2 There are no data centres or infrastructure located at the MSP Sites. All relevant infrastructure used by MSP staff to undertake their roles is either issued to them or made available to them via cloud services.
- 2.3 To ensure both the safety of MSP staff and the continuity of the DSB Service, where an MSP Site becomes unavailable or inaccessible for any reason, the MSP staff shall be enabled to work remotely. The MSP regularly tests this approach. The DSB shall also undertake an annual MSP Site BCP test with all MSP staff working remotely at the same time.
- 2.4 The DSB shall provide status updates on its website in the event that the BCP at MSP Sites is invoked.

3 BCP Change Management

- 3.1 Should any aspect of BCP be invoked, the DSB shall work with the TAC to agree the approach in relation to any resulting IT changes required to the DSB Service. If required, the TAC may recommend either a period of "heightened awareness" (as described in paragraph 3.1(a)) or a period of "change freeze" (as described in paragraph 3.1(b)) to be established.
 - (a) Heightened awareness period

If the TAC recommends a period of heightened awareness, the DSB shall introduce additional governance measures to review all IT changes, both planned and emergency, before proceeding with such changes. The DSB shall attempt to ensure that any IT changes made do not require End Users to make changes at the same time as the DSB. However, it is recognised that some organisations may wish to make changes, for example to adopt the new functionality being added. Where IT changes are proposed that require End Users to make changes at the same time as the DSB, further guidance may be sought from either the Product Committee (as defined in the DSB Governance Policy) or the TAC, or both.
 - (b) Change freeze

If the TAC recommends a change freeze, the DSB shall not undertake any planned IT changes. Only essential IT changes that are required to keep the system running shall be permitted and such changes shall be subject to additional governance measures.

¹ <https://www.anna-dsb.com/technology-advisory-committee/>

² <https://www.anna-dsb.com/download/technology-advisory-committee-charter/>

³ <https://www.anna-dsb.com/>

4 Pandemic

- 4.1 The MSP maintains a business continuity plan to ensure that essential functions and services during a pandemic are maintained.

5 High Availability

- 5.1 The DSB Service is built and configured on the Amazon Web Services public cloud (“**AWS**”) for “high availability” within an AWS Region.
- 5.2 The AWS service is built with three Availability Zones (“**AZ**”) present in each AWS Region. Automatic server-side failovers and load balancing are present as per AWS’ best practice to ensure a highly available environment.
- 5.3 An AZ comprises one or more discrete data centres with redundant power, networking, and connectivity in an AWS Region. All AZs in an AWS Region are interconnected with high-bandwidth, low-latency networking, over fully redundant, dedicated metro fibre, which provides high-throughput, low-latency networking between AZs. All traffic between AZs is encrypted. The network performance is sufficient to accomplish synchronous replication between AZs. AZs allow for easy partitioning between applications to ensure high availability. If an application is partitioned across AZs, companies are better isolated and protected from unforeseen events such as power outages, lightning strikes, tornadoes and earthquakes. AZs are physically separated from one another by a meaningful distance (i.e., many kilometres), although all AZs are within 100 km of each other⁴.
- 5.4 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.
- 5.5 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.
- 5.6 Server configurations shall be backed up securely.

6 Disaster Recovery

- 6.1 The DSB’s configuration in the primary AWS Region has been replicated to a secondary AWS Region. This secondary AWS Region is kept updated with the relevant software patches and versions that are applied to the primary AWS Region. The data is replicated in real time ensuring there are no database discrepancies between AZs and/or between AWS Regions.
- 6.2 The DSB encourages Users to utilise the network aliases that are provided to access the DSB Service, rather than directly accessing the underlying IP addresses. However, the DSB also provides the full set of primary and secondary IP addresses to ensure that Users can whitelist the full set of addresses. These two measures are aimed at ensuring that End Users do not need to make changes in the event of the DSB invoking its DR plan.
- 6.3 The DSB’s DR plan shall be invoked if:
- (a) two or more of the AZs in the AWS Region fail; or
 - (b) there is a loss of an entire AWS Region.
- 6.4 Recovery Time Objective (RTO)

The DSB aims to have the DSB Service running within 4 hours of the decision to invoke the DR plan. This RTO was agreed following consultations with the industry and the TAC.

⁴ https://aws.amazon.com/about-aws/global-infrastructure/regions_az/

6.5 Recovery Point Objective (RPO)

- (a) The DSB aims to ensure that there is no data loss related to any transactions where the End User has already received a response.
- (b) Where the End User has not received a response to a transaction, the DSB requests End Users to resubmit the transaction when the DSB Service is established in the secondary AWS Region.
- (c) The DSB has agreed with the TAC to undertake an annual failover where the DSB services will be failed over from the primary to the secondary region. The DSB will run from the DR region for a two-week period and then fail back to the primary region. Failover and failback will take place during the DSB's downtime window. During the failover period, the DSB's primary region will be configured to act as the DSB's secondary region. This is to prevent the risk of data loss in the event of an issue with the (now) primary region.

7 Third Party Data Vendor BCP Dependencies

- 7.1 The DSB selects its vendors by assessing a wide range of criteria, including their organisational maturity and public BCP attestations. All critical infrastructure providers must be able to supply suitable assurances prior to engagement and integrate successfully with DSB BCP activities if this is required. Periodic review and management of BCP activities of these suppliers is a part of the DSB's annual BCP review.
- 7.2 The DSB publishes a [list of its subcontractors](#)⁵ used in the provision of the DSB Services (and their locations) on its website, together with details of the DSB's own service locations. Changes to this list will be made on the same basis as set out in clauses 1.2 to 1.4 of the Main Terms.

⁵ <https://www.anna-dsb.com/subcontractors/>