ASSETBANK

T 01273 923150
E info@bright-interactive.co.uk
W assetbank.co.uk

INFRASTRUCTURE BACKUP AND DISASTER RECOVERY

Policy version number 1.2 22nd October 2020

1. Introduction

1.1. This policy outlines the approach of Bright Interactive Limited (Bright) to the implementation and management of backups and disaster recovery for Asset Bank clients on our shared or dedicated hosting infrastructure.

1.2. This policy covers how Bright ensures the security and availability of backups and a robust disaster recovery approach through its approach to:

1.2.1. Roles, responsibility and access

1.2.2. Backup strategy

1.2.3. Disaster recovery

1.3. Bright's objective is to provide information on its approach for clients and clarity on the standards and responsibilities required of its employees.

1.4. Details of the access, storage and handling of data in Bright's Infrastructure Security Policy, Information Security Policy apply here to management of backup data.

1.5. The responsibility for the design and implementation and upkeep of this policy is held by the Information Security Manager. The ultimate responsibility for ensuring that information security is properly managed lies with the Directors. All staff are responsible for adhering to this policy and for reporting any security breaches or incidents to the Information Security Manager or a Team Leader.

1.6. This policy is reviewed and updated as it is deemed appropriate, but no less frequently than every 12 months.

2. Roles, Responsibility and Access

2.1. Bright has clear roles and responsibilities within the Infrastructure Team for the backup and restoration of client data, these are documented on the Company's internal Wiki and communicated to relevant parties.

2.2. Access to infrastructure systems and backup data is managed and restricted by the range of access controls documented in Bright's internal Access Control Policy and User Access Policy.

3. Backup Strategy

3.1. Clients on Bright's hosting platform are automatically included in its backup procedures upon installation of their Asset Bank instance.

3.2. Bright's backup strategy allows for all local files that are required to restore each Asset Bank being backed up to 3 geographically different locations.

3.3. Bright's primary backups use multiple approaches to ensure data can be easily and quickly accessed.

3.3.1. All digital asset files are stored in AWS S3 buckets and a backup set of buckets is created upon installation for the backup of asset files. All new uploaded assets are automatically synced across to the backup bucket where they are stored as an encrypted Glacier object.

3.3.2. The Asset Bank instance is installed on an AWS EC2 server, allowing the EBS volume to be snapshotted every night. This snapshot captures all application files, and any asset files that have been shared using the applications integrated sharing functionality (e.g 'share by email' assets).

3.4. Secondary application and database backups are also created on a nightly basis and synced to a restricted area of the application's S3 bucket as an encrypted object. This backup is also synced to the application's backup bucket as an encrypted Glacier object.

3.5. Note that files in transient storage, for example, files that have not been fully imported into Asset Bank, or shared files, which have expiry dates, such as published lightboxes may not be backed up.

3.5.1. In a disaster recovery scenario, shared files can be regenerated from within the application

4. Data Deletion

4.1. Application and asset backups are synced incrementally and any backup data will be accessible for a minimum of 90 days after its creation.

4.2. When hosted data is no longer needed, eg due to termination of a contract, the Company follows best practice guidelines for the proper destruction of the data (NIST's Guidelines for Media Sanitization (Special Publication 800-88 Revision 1 - December 2014)) for all media over which Bright has the required control.

4.3. Bright follows standard practice for the deletion of assets from AWS S3.

5. Backup Testing

5.1. The Company implements an annual program of backup testing to ensure that backed up data will be available when required.

5.2. After each series of testing a review is undertaken and any areas for improvement identified and implemented as appropriate.

5.3. The backup testing programme covers the full range of scenarios that may result in the loss of client data. This ranges from the accidental deletion of a small amount of data by a client up to the loss of an entire application server or AWS S3 bucket.

5.4. A record of the testing, review and any actions taken is documented as part of each testing cycle and made available on the internal Wiki

5.5. Backup procedures are designed to fit into the Bright Interactive Disaster Recovery plan and, as such, are a service included in the contracted hosting costs.

5.6. Backups can be restored in response to a client request, for example where data has been deleted accidentally by a client administrator. All work required to restore data or applications upon client request will be charged at our prevailing support rates.

6. Disaster Recovery

6.1. Bright has implemented a range of processes to support recovery of client data and applications in the event of critical failures.

6.2. An outage of any application or service is always addressed with the highest priority within the Infrastructure team.

6.3. 24/7 incident monitoring across the infrastructure ensures that any failure within the application, or a service related to the application, is identified and reported directly to the Infrastructure team.

6.4. Upon receiving notification of an incident, members of the Infrastructure team are to make themselves available to attend to the issue, with a target start time of 60 minutes for beginning work on the issue

6.5. Upon an issue being reported the infrastructure team follow this process:

6.5.1. Immediate troubleshooting and investigation with the objective of resolving the issue on the live server, in line with the Client Service Incident Management Policy.

6.5.2. Where the failure cannot be rectified within 3 hours, move to restore the application from the backup (see backup policy). An AWS EC2 snapshot of the server will be restored to a new EC2 instance in our AWS VPC.

6.6. Bright's Service Level Agreement for disaster recovery provides for a critical failure of an Asset Bank being rectified within 1 business day of failure. Nevertheless Bright commits to taking all efforts to resolve critical failures as

quickly as possible. For example we aim to restore an Asset Bank to a new EC2 instance within 4 hours.

6.7. In the rare event that there is a complete loss of an application's production asset bucket, Bright will thaw a backup of the original files from the backup Glacier bucket in AWS.

6.8. The Company has a Client Service Incident Management Process which must be followed for every infrastructure service incident. This Policy gives a framework for the investigation and reporting of the issue as well as the identification of mitigating actions to prevent the recurrence of a similar issue in the future, see Bright's Client Service Incident Management Process for details.

6.9. All aspects of the Disaster Recovery Plan are documented on the Company's internal Wiki and communicated to relevant personnel.

Version control

VERSION	DATE	AUTHOR	RATIONALE
1	23/03/2018	InfoSec Manager	First release
1.1	21/05/2020	InfoSec Manager	Annual review and minor amends
1.2	22/10/2020	InfoSec Manager	Addition of transient storage backup caveat