

Magiq Limited

Magiq Security and Back-up Policy

1 Data Types and Data Policy Objectives

This document discusses the types of data collected, processed, created and reported by the Magiq™ systems. It classifies these data types by their characteristics, and describes the processes necessary to manage each type of data in terms of back-up, security, retention and recovery.

1.1 Types of data

The data gathered and processed by a Magiq™ system can be classified into these three types:

- **Raw data** – the data as it is received from the Magiq™ file
- **Processed visitor data** – the processed usage and visitor profile data needed to drive Prospect, Retain and Smart.
- **Configuration data** – the configuration and report settings data that relates to a customer's Magiq™ instance.

These three sets of data are, for the purpose of this document, the defined data types.

1.2 Objectives of data management policy & procedures

Each type of data has differing values and lifetimes. Therefore the policies and processes for the backup of each Defined Data Type are optimized to meet the value and lifetime of the Defined Data Type.

1.3 Backup Considerations

Raw data – this data is ephemeral in nature and of transient interest to the system and its users. Once it has been processed and an action taken by a product, whether it be a site change, or for storage in the visitor's data profile, it is no longer of use and the system will discard it. This raw data is never stored in a database, and only exists in memory or cache.

Processed visitor data – As this is of long term value to the system and customer. Magiq™ will use all reasonable endeavors to retain this data for the life of a Magiq™ customer contract. The policies therefore define a schedule of regular snap-shot backups that will be taken of this data within the cloud.

1.4 Security Considerations

The information security requirements reflect both the commercial sensitivity of the data and the need to reflect the requirements of applicable data protection legislation (e.g. The Data Protection Act 1998 in the United Kingdom)

Magiq's policies and procedures described in this document are designed to provide a secure environment capable of meeting the needs of the Defined Data Types.

1.5 Contingency Considerations

The policy reflects the fact that for most customers the services provided are not part of the customer's mission-critical operational procedures, and therefore it is not necessary, or cost effective, to provision specific disaster recovery systems. The policies therefore recognize this fact and utilize the fact that Magiq™ operates within the Amazon Elastic Compute Cloud, which physically exists within multiple hosting facilities and has a resilient infrastructure.

2 Policies and procedures

The following sections describe the specific policies and procedures implemented to provide the levels of backup, security and continuity defined in the above objectives and considerations.

2.1 Security & Backup Policy

2.1.1 Raw Data

The policy relating to this is as follows:

The data should be processed as soon as the application allows. The data is entirely transient. Magiq™ does not undertake any backup processing for this Defined Data Type.

2.1.2 Processed Visitor Data

The policy relating to this is as follows:

The data of this Defined Data Type is written to an Amazon EBS (Elastic Block Store) volume, which is an off-instance storage system that persists independently from the life of the server instance.

Amazon EBS volumes are highly available, highly reliable volumes that are provided with the ability to create point-in-time consistent snapshots of the volume, that are stored within Amazon S3 (Simple Storage Service) and automatically replicated across multiple availability zones. A snapshot of the Amazon EBS volume will be taken once a week.

2.1.3 Configuration Data

The policy relating to this Defined Data Type is as follows:

All configuration data is backed up to the associated Amazon EBS (Elastic Block Store) volume, which is an off-instance storage system that persists independently from the life of the server instance.

Amazon EBS volumes are highly available, highly reliable volumes that are provided with the ability to create point-in-time consistent snapshots of the volume, that are stored within Amazon S3 (Simple Storage Service) and automatically replicated across multiple availability zones. A snapshot of the Amazon EBS volume will be taken once a week.

2.2 Systems Security Policies

These policies are designed to address the following considerations:

- Protection of data during collection (from client's browser to Magiq™ instance)
- Protection of data from illegal access on Magiq™ instance configuration interface
- Protection of data from illegal access via Magiq™ instance reporting interface

2.2.1 Data capture and transmission security

Magiq's servers will automatically encrypt or obscure all data collected from users' browsers while browsing an instrumented site.

The encryption technique is determined at run-time by the Magiq™ file running in the client's browser as part of the page content as follows:

- If the page is https: (SSL) then the data is encrypted using SSL techniques using an SSL license held on the Magiq™ instance.
- If the page is http: and therefore should not contain any secure information or secure forms, then the data will be obfuscated via a light-weight proprietary encryption technique.
- If the page is http: but does contain secure content (e.g. Secure form posts) it is classed as a "mixed mode page". The data will be encrypted and returned to the Magiq™ instance via SSL encryption techniques.

2.2.2 In-Page change information transmission

- If the page is https: (SSL) then the data is encrypted using SSL techniques using an SSL license held on the Magiq™ instance.

- If the page is http: and thus should not contain any secure information or secure forms then the data will not be encrypted.

2.2.3 System internal communication

Data transferred between the capture system, processing system, database and in-page change system is all internal to the instance(s) and not visible from the internet.

2.2.4 Physical Security

Because of the nature of the Amazon EC2 (Elastic Compute Cloud) instance used by Magiq, no physical access to the hardware can be obtained by Magiq™ staff or customers. Details of Amazon's security can be seen in the Amazon AWS Security White-paper - http://s3.amazonaws.com/aws_blog/AWS_Security_Whitepaper_2008_09.pdf

2.2.5 Operational Security / Integrity

Magiq™ operates automated monitoring processes which operate 24x7x365 with SMS alerts to members of the Operations team. These monitor the operation of key processes, services and databases.

2.2.6 Internet / Hacking protection

- Magiq™ provides access only to TCP ports essential for operational interfaces.
- Magiq™ utilizes normal password protection systems at operating systems, Magiq™ instance and database levels.
- Magiq™ does not provide direct access to Raw Data or Processed Visitor Data. Configuration data is only available to the customer via the Magiq™ interface.
- Magiq™ interfaces are password protected and utilize SSL protocols where required.
- Magiq™ services report failed attempts to access administration consoles.

2.2.7 Access control

- Passwords and user ID access to the Magiq™ interfaces will be provided to identified customer representatives for use by their staff or contractors. These will only be provided to the support or administration interfaces nominated by the client and to approved Magiq™ support and operations staff.
- Passwords and user IDs will not be transmitted together.
- No direct access to the Magiq™ instances is provided to non-Magiq™ personnel.
- Passwords are set by the customer on sign-up and should be a minimum of 6 characters, and be composed of case-sensitive non-obvious words, which should include a mixture of numeric and alphabetic characters. Passwords may be reset by the customer at any time.

2.3 Organizational Measures

2.3.1 Non-disclosure agreements

Staff are controlled via the security agreements signed with their employment contracts. If external consultants are used their contracts include extensive NDA and security agreements.

2.3.2 Recruitment procedures

Magiq's HR manager is responsible for recruitment. All prospective candidates will be interviewed (as a minimum) by the HR Manager, their line manager and a company director. Magiq™ obtains two references for all employees prior to engagement.