Reward Gateway Encryption Policy

Classification – Confidential

March 2019 – Version 1.6

265 Tottenham Court Road
London
W1T 7RQ
UK

Table of contents

Document purpose

Reward Gateway must use encryption in order to reduce the risk of exposing personal information. The purpose of this policy is to provide guidance on the use of encryption and algorithms that have received substantial public review, as well as being proven to work effectively.

General approach

This policy applies to all software and servers operated by Reward Gateway, specifically applying to:

- All software written by Reward Gateway.
- All data hosted at Amazon Web Services (AWS), including backups.
- Connections made to and from the cloud at AWS.
- Configuration settings and/or keys related to securing connections.
- Single sign-on clients.

Definitions

Term	Definition
Proprietary Encryption	An algorithm which has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.
Symmetric Cryptosystem	A method of encryption in which the same key is used for both encryption and decryption of the data.
Asymmetric Cryptosystem	A method of encryption in which two different keys are used – one for encrypting and one for decrypting the data, e.g. public-key encryption.
Hash Function	A hash function is any algorithm that maps data of arbitrary length to data of a fixed length.

Policy

1. Selection and procurement of encryption facilities will only be performed by the Chief Technical Architect.
2. All Reward Gateway computer devices that can be used to administer AWS environment must have Reward Gateway approved encryption software installed prior to their use within Reward Gateway. In addition to encryption

software, the device must also be password protected and have up to date anti-virus software installed – see Anti-Virus Policy.

3. Where Strictly Confidential and Confidential information is transmitted through a public network (for example the Internet) to the production environment, the information must be encrypted first or sent via a secure channel. For example, via an TLS or SSH connection.

Approved algorithms and protocols

Proven, standard algorithms and protocols should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. Reward Gateway's algorithm list and key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose.

Symmetric algorithms

- Advanced Encryption Standard (AES) – Minimum encryption key length of 256 bits must be used for data in transit and at rest.

Asymmetric algorithms

- Rivest, Shamir & Adelman (RSA) – Minimum private key length of 2048 bits.

Hashing algorithms

- SHA-512
- bcrypt

Encryption protocols

- TLS (Transport Layer Security)
- SSH (Secure Shell)
- S/MIME (Secure Multipurpose Internet Extension)

Exceptions

Reward Gateway work with various suppliers and partners to deliver the services to end-users. Not all of these partners will be able to comply with the requirements of Reward Gateway's encryption standard.

In the event that a partner cannot comply, it should be treated as a general exception and a risk assessment conducted.

Key management

The following practises should be applied to any encryption keys:

- As far as possible, the management of the keys should be fully automated.
- Private keys are personal and disclosure to another employee or a 3rd party is deemed as compromise and should be reported.
- Keys at-rest must be encrypted and password protected. The only exception being the Master Key is printed and kept in a secure location.
- Keys should be rotated on a periodic basis depending on their function but this should be for no longer than 2 years.

All keys for access to systems containing sensitive information, such those in AWS, are controlled by the DevOps engineer.

Revision history

Rev	Date	Author	Description	Approved	Date
1.0	24.03.2014	Will Tracz	Initial draft.	Richard Hurd-Wood	28.03.2014
1.1	25.11.2014	Will Tracz	Apply ISMS labelling.	Richard Hurd-Wood	30.11.2014
1.2	10.08.2015	Will Tracz	Updated format and section headings.	Richard Hurd-Wood	22.08.2015
1.3	20.05.2016	Ivan Dichev	Minor update.	Richard Hurd-Wood	27.05.2016
1.4	01.03.2017	Liam Jones	Rebrand and general clean.	Will Tracz	03.03.2017
1.5	29.06.2018	Asen Varsanov	Full review and update.	Will Tracz	01.07.2018
1.6	07.03.2019	Asen Varsanov	Move to AWS from The Bunker	Will Tracz	10.03.2019