TORQUE
SOFTWARE

# LIGHTHOUSE TECHNICAL GUIDE

# CONTENTS

# INTRODUCTION

Lighthouse from Torque Software is a Software as a Service (SaaS) application used by Government entities to manage governance, compliance, and assurance activities. This document provides information about Lighthouse to assist client technical support.

# DEVELOPMENT PLATFORM

The Lighthouse development platform is Microsoft .NET 4.5 and Microsoft SQL Server. Third party controls have been used to develop the application (sourced from DevExpress), however these are all native .NET source code.

# ARCHITECTURE

Lighthouse is a two-tier application with the ASP.NET application component executing on Microsoft IIS. The database is Microsoft SQL Server.

# HOSTING

The Lighthouse application is hosted using Amazon Web Services (AWS) located in Sydney, Australia.

# IRAP CERTIFICATION

The AWS hosting environment and the Lighthouse application are IRAP certified and meet all Australian Federal Government cyber security requirements, including hosting of all data in Australia.

All AWS services utilised are certified to at least PROTECTED level.

# USER ACCESS SECURITY

Lighthouse provides three user access security options.

## VANguard Federated Authentication Service - Single Sign-On

VANguard is provided by the Department of Industry, Science, Energy and Resources and is recommended for Australian Federal Government entities wishing to obtain authentication services for internet applications.

The VANguard Federated Authentication Service allows users logged on to their own Australian Federal Government entity's network to authenticate and then use web applications such as Lighthouse. Authentication occurs transparently without additional credentials or software being required on the user's computer.

### Microsoft Azure AD - Single Sign-On

Lighthouse supports Microsoft Azure AD single sign-on. Authentication occurs transparently without additional credentials or software being required on the user's computer.

### Username/Password Authentication

User identity is assured through standard username and password protocol; passwords are encrypted within the database using AES encryption. Password complexity requirements can be set within the application, and multi-factor authentication (MFA) can be configured.

Failed logon attempts are logged and available for viewing within Lighthouse. Lighthouse can be configured to lockout accounts after a set number of failed login attempts.

## INFORMATION TRANSFER SECURITY

Lighthouse supports obtaining user and organisation structure information from client systems via CSV file transfer. The transfer process can be automated or performed manually.

#### Automated Transfer

Automated transfer is performed via Secure File Transfer Protocol (SFTP) and can execute overnight or other times as appropriate.

#### Manual Transfer

CSV files can be manually uploaded directly from a protected network into Lighthouse by suitably authorised administrators.

## BROWSER SECURITY

Lighthouse runs over TLS (commonly known as HTTPS), ensuring an encrypted communication channel between the client browser and Lighthouse server.

Lighthouse uses cookies as standard to maintain authentication state (industry standard). Using cookie-based authentication over URL-based ensures that only the local machine containing the cookie can access the authenticated session.

To learn more about Torque Software, contact us on 1300 795 581 or visit www.torquesoftware.com.au.

TORQUE SOFTWARE