Lighthouse
GRC

Cyber Security Guide

Lighthouse GRC

Table of Contents

Introduction

LighthouseGRC Limited is a governance and compliance software system delivered via a Software as a Service (SaaS) platform. LighthouseGRC is used within the Australian Federal Government, state governments and similar organisations. More information about LighthouseGRC Limited and LighthouseGRC is available at the LighthouseGRC Limited Web Site.

The LighthouseGRC Cyber Security Guide provides essential information for use by IT professionals who are supporting their organisation's governance and compliance business objectives (both legislative and organisational policy), by implementing and using LighthouseGRC by LighthouseGRC Limited.

Information Security Registered Assessors Program (IRAP)

The LighthouseGRC cloud hosting platform and the LighthouseGRC software application have both been assessed under **IRAP** to comply with the Australian Federal Government **Information Security Manual** and the **Protective Security Policy Framework**.

LighthouseGRC Cloud Hosting Platform

LighthouseGRC is hosted on the Amazon Web Services (AWS) EC2 Cloud located in Sydney, Australia. Amazon runs many of the largest and most security-conscious sites on the internet. For more information on Amazon's EC2 Cloud, visit https://aws.amazon.com/ec2/

All AWS services utilised are certified to at least PROTECTED level. Supporting documentation is available as follows.

- Amazon Web Services IRAP Letter of Compliance

Gateway

Each Amazon VPC is a distinct, isolated network within the cloud; network traffic within each Amazon VPC is isolated from all other Amazon VPCs. At creation time, an IP address range is selected for each Amazon VPC. An Internet gateway, virtual private gateway, or both may be created and attached to establish external connectivity, subject to the appropriate controls.
Secure communication between client and server is ensured via TLS certificates.

Identity and Access Management

Identity and Access Management (IAM) is managed through Amazon's AWS IAM. See http://aws.amazon.com/documentation/iam/ for more information.

LighthouseGRC Software Application

The LighthouseGRC software application IRAP assessment letter is available at LighthouseGRC Software Application IRAP Assessment. Detailed assessment results are available from LighthouseGRC Limited on request.

The LighthouseGRC development platform is Microsoft .NET 4.5 and Microsoft SQL Server. Third party native .NET source code controls have also been used to develop the application (sourced from DevExpress). LighthouseGRC is a two-tier application with the ASP.NET application component executing on Microsoft IIS.

Security Clearances

All LighthouseGRC Limited staff which have access to client instances have been issued with a Commonwealth Government Security Clearance. Those staff with heightened access to customer source data and system infrastructure are required to hold an NV1 clearance or higher.

Access is only granted where necessary for client support services. Client data is only accessed when required for client support activities.

User Access Security

LighthouseGRC provides three user access security options.

Microsoft Azure AD - Single Sign-On

LighthouseGRC 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 LighthouseGRC. LighthouseGRC can be configured to lockout accounts after a set number of failed login attempts.

Browser Security

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

LighthouseGRC 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.

Cyber Security Updates

LighthouseGRC Limited keeps up to date with all cyber security matters by maintaining membership with the following groups.

- The Australian Cyber Security Centre (Australian Signals Directorate, Department of Defence) as a Network Partner
- The Australian Information Security Association

LighthouseGRC Limited has also engaged expert cyber security consultants who constantly monitor our cyber security processes to ensure current industry requirements and best practice are met.

Help Desk

LighthouseGRC Limited help desk support services are available to client IT support personnel and LighthouseGRC system administrators to report possible cyber security incidents at any time by emailing info@lighthousegrc.uk

LighthouseGRC Limited C/O Fladgate LLP. 16 Great Queen Street London, WC2B 5DG

Email: info@lighthousegrc.uk

https://Lighthousegrc.uk