veezu.

INFORMATION SECURITY POLICY STATEMENT

Information is an important business asset of significant value to Veezu Holdings Ltd. and needs to be protected from threats that could potentially disrupt business continuity.
Company's Information Security Policy has been written to provide a mechanism to establish procedures to protect against security threats and minimise the impact of security incidents as well as support the Group's Information Security Management System.

Our Information Security Management System (ISMS) is the means by which Veezu Holdings Ltd. (the 'Group') satisfies the requirements of BS ISO/IEC 27001: 2013 with regard to the Group's overall business risks. It specifies the requirements for the implementation of security controls, customised to the needs of the Group or to specific parts thereof.

The scope of our registration is: THE PROVISION OF PRIVATE HIRE SERVICES

The Group is obliged to ensure that the established controls are completely understood by its employees and that its procedures and control documentation are implemented and maintained at all times. All of the components of this ISMS are periodically and systematically reviewed by both internal and external audit procedures.

A nominated member of staff has been appointed by the Group's Chief Executive Officer to be responsible for the control of all matters relating to the implementation, control and continuing audit of these procedures.

The implementation and continuing control of the ISO 27001: 2013 requirements are fundamental to all work undertaken by Veezu Holdings Ltd. The procedures established shall be adopted and practised by all employees at every level in the Group's structure.

We have adopted the process approach for developing, implementing and improving the effectiveness of its ISMS and we are committed to:

1. Understanding business information security requirements and the need to establish policy and objectives for information security
2. Implementing and operating controls in the context of managing the Group's overall business risk
3. Monitoring and reviewing the performance and effectiveness of the ISMS
4. Continual improvement based on objective measures
5. Communicate throughout the Group the importance of meeting all relevant statutory and regulatory requirements specifically related to its business activities
6. Ensuring that adequate training and resources are determined and provided to monitor and maintain the ISMS.

Each employee is responsible for his/her adherence to the principles of the Group's Information Security Policy.

The Group will monitor the effectiveness of this policy and its general compliance within the organisation.

Nathan Bowles
Chief Executive Officer

amazing journeys.