Document Number	AS-QHSSE-PR-04
Version Number	02
Prepared By	V. PSELVEM
Approved By	R. BHOJ
Approved Date	01 JAN 2020

TITLE: SECURITY POLICY

DOCUMENT NUMBER: AS-QHSSE-PR-04

APPROVING AUTHORITY: R. BHOJ

REVISION HISTORY

Version Number	Summary of changes made	Approved By	Approved Date
01	Policy released	R. BHOJ	01 JAN 20
02	Change to the company group member list	R. BHOJ	05 AUG 20

This policy applies to the following group of companies (hereinafter collectively and individually referred to as the COMPANY):

Aroona Solutions Sdn Bhd. – Malaysia

Aroona Solutions Integrated Sdn Bhd. – Malaysia

Aroona Energy Solutions (M) Sdn Bhd. – Malaysia

PT Aroona Solusi – Indonesia

Aroona Solutions Australia Pty Ltd. – Australia

Blueline Solutions – India

Deepsea Offshore and Marine Pte Ltd. – Singapore

Document Number	AS-QHSSE-PR-04
Version Number	02
Prepared By	V. PSELVEM
Approved By	R. BHOJ
Approved Date	01 JAN 2020

SECURITY POLICY

The management of information security and information systems assists in ensuring a secure workplace for all COMPANY team members. The management of information security is applicable to all IT devices owned or supplied by the COMPANY in addition to all team member owned networks, computers or mobile devices used to conduct COMPANY business.

All team members are to consider the security of COMPANY information and how it is handled. This includes, but is not limited to, mobile and remote working, password security and cloud storage.

COMPANY team members must adhere to below points:

- Information will be protected in accordance with all applicable legislation.
- Measures must be taken to ensure information is protected against unauthorised access.
- Team members must not divulge their IT passwords to anyone for any reason.
- Access IT accounts of team members who no longer work for the COMPANY will be cancelled immediately.
- Reasonable personal use of COMPANY facilities is permitted, but only where it does not interfere with Aroona Drilling business or contravene any COMPANY policies.
- External data storage facilities should only be used to store COMPANY data.
- COMPANY data should not be stored in cloud storage other than that provided by the COMPANY.
- Personal equipment should not be connected to the COMPANY network.
- Unacceptable IT usage may be dealt with under disciplinary procedures.
- All software will be actively managed to ensure it is up to date and secure.
- Software licences must be in place before usage to minimise risk to the IT system.
- Software that creates significant risks to the network such as games and instant messaging are not to be utilised on the COMPANY network.
- Remote work access is permitted from both personal and COMPANY owned devices. These devices must be password protected and secure.

All team members should be aware that the COMPANY in accordance with relevant legislation, may access records of use of internet, email or telephone to conform to any applicable legislation, to check for operational effectiveness and to detect unauthorised use.