Information security is the protection of information and supporting systems from a wide range of threats in order to ensure business continuity, minimise operational risk, and maximise return on investments and operational opportunities.

This policy is aligned with relevant regulatory frameworks and standards that JobQuest operates within to facilitate effective delivery of our services and meeting the expectation of various funding bodies and regulatory authorities.

These specifically include the Information Security Plan and the Date Security Breach Response Plan and the Cyber-Security Incident Plan.

Data, information and the underlying technology systems are essential assets to JobQuest, and provide vital resources and tools to staff and service users. They need to be suitably protected.

Information security will be achieved by implementing a suitable set of controls in accordance to the risk profile. These control measures are documented in the Information Security Plan and include processes, organisational structures and software and hardware functions. These controls will be established, implemented, monitored, reviewed and improved, where necessary, to ensure that specific security and objectives of JobQuest are met.

JobQuest is committed to providing a secure, yet open information environment that protects the integrity and confidentiality of information without compromising access and availability meets its obligations with applicable laws, regulations, and standards.

The Policy covers the continued availability of information and the information environment to support JobQuest's business activities; including the implementation of appropriate controls to protect information from intentional or accidental disclosure, manipulation, modification, removal or copying.

JobQuest is responsible for safeguarding the organisation's information environment and information resources against security threats. JobQuest discharges its responsibilities through the following and the set of measures outlined in this Policy and more specifically in the Information Security Plan, the Date Security Breach Response Plan and the Cyber-Security Incident Plan and include:

1. Defining roles and responsibilities and establishing clear lines of accountability;
2. Protecting JobQuest's information assets against internal and external threats (e.g. security breach, loss of data);
3. Ensuring that JobQuest complies with applicable laws, regulations, and standards;
4. Identifying and treating security risks to the organisation's information environment through appropriate physical, technical and administrative channels;
5. Responding effectively to breaches, threats and vulnerabilities; and
6. Developing best practices for effective information security across the whole organisation.

User Responsibilities:

1. Users must abide by all relevant laws and all JobQuest procedures and protocols – more specifically the Information Security Plan and the IT, Internet, Email and Social Media Protocol;
2. Users are expected to take responsibility for developing an adequate level of information security awareness, education, and training to ensure appropriate use of the information environment;
3. Users may only access information needed to perform their authorised duties;
4. Users must protect the confidentiality, integrity and availability of JobQuest's information and data;
5. Users may not in any way divulge, copy, release, sell, loan, alter or destroy any information, except as authorised by the relevant JobQuest delegate;
6. Users must safeguard any physical key, ID card or online and network account that enables access JobQuest information. This includes maintaining appropriate password creation and protection measures;
7. Any activities considered likely to compromise sensitive information must be reported to the relevant supervisor or to the management of JobQuest; and
8. Users are obliged to protect sensitive information even after separation, termination or resignation from JobQuest.

Delegated Authority

In addition to complying with the requirements listed above for all staff, contractors and volunteers, senior management staff must:

1. Ensure that program specific procedures support the objectives of confidentiality, integrity and availability defined by this policy, and that all JobQuest policies and procedures are followed;
2. Ensure that controls and safe guards are effectively communicated to those who use, administer, capture, store, process or transfer the information in any form, physical or electronic; and
3. Ensure that each staff member is provided with training and therefore understands his or her information security related responsibilities.
4.

Risk Assessment and Treatment

Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the operational damage likely to result from security failures. The results of the risk assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls to protect against these risks.

2nd July 2020

Ka Chan
Chief Executive Officer