DSA-QAG INFORMATION SECURITY POLICY

1. INTRODUCTION

DSA-QAG is an audit organisation, as such, we collect sensitive organisational data. This includes, but is not limited to key performance indicator (KPI), annual statistics and audit data.

It is DSA-QAG's policy that the information it manages, in both electronic and hard copy, is appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information.

We will do this in ways that are appropriate and cost effective. This will help enable DSA-QAG to fulfil its mission, protect the interest of all parties and ensure that a high quality service can continue to be offered to our registered practitioners.

2. SECURITY OBJECTIVE

Our security objective is to protect DSA-QAG and its registered practitioners from security problems that might have an adverse impact on operations and professional standing.

Security problems can include confidentiality (the wrong people obtaining information), integrity (information being altered without permission, whether deliberate or accidental) and availability (information not being available when it is required). The widest possible definition of security will be used to include all types of incident that impact the effective use of information. This includes performance, consistency, reliability, accuracy and timeliness.

3. PRINCIPLES

3.1 Approach

- We will use all reasonable, appropriate, practical and effective security measures to protect our important processes and assets in order to achieve our security objectives.
- We will continually examine ways in which we can improve our use of security measures to protect and enhance our business.
- As a responsible organisation, we will protect and manage our information assets to enable us to meet our contractual, legislative, privacy and ethical responsibilities.
- We will ensure that our data are held safely so that their continued validity is not questioned.
- We will engage with our practitioners in order to ensure our approach to data security is understood and supported by our stakeholders.

3.2 Responsibilities

Everyone within DSA-QAG who uses our information will be responsible for protecting our information assets, systems and infrastructure. They will, at all times, act in a responsible, professional and security-aware way, according to the principles in this policy and the Central Administrative Units' operational procedures and practices.

Everyone will protect information assets that are entrusted to them, whether such protection is required contractually, legally, ethically or just out of respect for other individuals or organisations. An individual may not put the intellectual and information assets of others at risk through carelessness or selfishness.

All staff members of DSA-QAG are responsible for identifying security shortfalls in our existing security practices and/or improvements that could be made. These should be reported to DSA-QAG's CEO.

All staff members of DSA-QAG who have supervisory responsibility are expected actively to coach and encourage best practice amongst their supervised staff or students.

Practitioners who become aware of any discrepancies gaps in DSA-QAG's information security should be encouraged to report this as soon as is possible to the DSA-QAG's CEO so that action to address the discrepancies may be taken promptly.

3.3 Practices

All staff members of DSA-QAG will be accountable for their actions and all actions will be attributable to an identified individual.

All information (including third party information) will be protected by safeguards and handling rules appropriate to its sensitivity and criticality.

DSA-QAG will ensure that its activities can continue with minimal disruption or other adverse impact, should it suffer any form of disruption or security incident. Actual or suspected security incidents will be reported promptly to the Operations Manager and CEO, who will ensure that the incident is managed to closure, and analyse it for policy updates. Documented Procedures and standards, education and training, will supplement these Principles.

3.4 Security Policy Review

The policy will be reviewed on an annual basis, or as required, for completeness, effectiveness and usability. Effectiveness will be measured by DSA-QAG's ability to avoid security incidents and minimise resulting impacts, together with a process for benchmarking security maturity with other similar establishments.

All staff members of DSA-QAG are responsible for identifying ways in which the Security Policy might be improved. Suggestions for improvement should be sent to the Operation Manager. Unless immediate changes are required, suggestions will be discussed at the annual review of the Policy.

3.5 Policy Awareness

DSA-QAG will send an electronic copy of this policy to each new staff member joining the organisation and keep the current edition readily available on the organisation's public website. Following each review, the URL of the updated policy will be sent to each team member. All staff members are expected to be familiar with, and to comply with the Security Policy at all times. The Data Protection Office will, in the first instance, be responsible for interpretation and clarification of the Security Policy. Staff members requiring education about any aspects of this policy should discuss their needs with the Operations Manager.

3.6 Applicability and Enforcement

This Policy applies to all staff members of DSA-QAG. Compliance to the Policy will be part of the contract of employment.

Failure to comply with the Security Policy could harm DSA-QAG’s ability to achieve its mission and/or damage the professional reputation of the organisation. It will, in the ultimate sanction, be treated as a disciplinary matter. The CEO will be responsible for all decisions regarding the enforcement of this policy, utilising the disciplinary procedures as appropriate.