

I.G. Global Services Ltd.

INFORMATION SECURITY POLICY

1. INTRODUCTION

I.G. Global Services Ltd. is heavily reliant on using information in whatever form and where ever it exists to trade in its relevant areas. Next to its people, information is our most important asset. Without it we would not be able to function effectively as a Company.

Because of its importance, we recognise that this organisation must protect its information assets. We will do this in ways that are appropriate and cost effective.

This will help enable the Company to fulfil its mission, protect its reputation and ensure that a high quality service can continue to be offered to our clients.

Our ability to exploit and gain advantage from information will enable us to maintain and improve our reputation and ensure that we meet our strategic business and professional goals.

2. SECURITY OBJECTIVE

Our security objective is to protect the Company from security problems that might have an adverse impact on our 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 BS7799: Code of Practice for Information Security Management as a framework for guiding our approach to managing security.
- 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.

3.2 Responsibilities

Everyone within the Company or 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.

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.

We recognise the right to individual freedom, but freedom also requires responsibilities. An individual may not put the intellectual and information assets of others at risk through carelessness or selfishness.

All members of the Company are responsible for identifying security shortfalls in our existing security practices and/or improvements that could be made. These should be reported to the Company's Health & Safety Manager.

All members of the Company who have supervisory responsibility are expected actively to coach and encourage best practice amongst their supervised staff.

The Managing Director is responsible and accountable for ensuring that our security objective is achieved. The Managing Director of I.G. Global Services Ltd. is committed to pursuing appropriate programmes, activities and actions that contribute to achieving our security objective and that are consistent with this security policy.

The Departmental Managers will meet at least biannually to take informed decisions for the benefit of the majority. It will be held responsible by The Managing Director for achieving measurable progress.

The Managing Director is responsible for allocating sufficient resources so that the Company realistically can achieve its security objectives. This includes people, time, equipment, software, education and access to external sources of information and knowledge.

The Managing Director is the guardian of all information owned by the Company, having ultimate responsibility for ensuring that it is adequately protected and will delegate responsibility for approving and reviewing access rights to information to named, responsible individuals.

3.3 Practices

Using risk analysis techniques, we will identify our security risks and their relative priorities, responding to them promptly and confidently, implementing safeguards that are appropriate, effective, culturally acceptable and practical.

To promote better sharing and exploitation of information, all members of the Company will have free access to internal information, including details of security measures employed, unless there is a clear need to restrict their access.

All members of the Company 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.

Company information will only be disclosed to third parties when their need to know has been consciously assessed and with clear undertakings on its subsequent use. Information owners will be responsible for identifying to whom their information may be released and on what terms. Disclosure of personal information is subject to law.

The Company will ensure that its activities can continue with minimal disruption or other adverse impact, should it suffer any form of disruption or security incident.

Compliance with the Policy will be monitored on a regular basis by Internal Audit to be carried out by The Company's Health And Safety Manager.

3.4 Security Policy Review

The Director of I.G. Global Services Ltd. owns this Policy and is committed to the implementation of it. The policy will be reviewed annually for completeness, effectiveness and usability. Effectiveness will be measured by the Company's ability to avoid security incidents and minimise resulting impacts, together with a process for benchmarking security maturity with other similar establishments.

It is required that year on year there will be an improvement in security maturity within the Company. This improvement will be measured and reported on during this annual review, together with identification of, and approval for, planned improvements during the following twelve months.

The Managing Director will sign off all new versions of the Security Policy. All members of the Company are responsible for identifying ways in which the Security Policy might be improved. Suggestions for improvement should be sent to the Managing Director of I.G. Global Services Ltd. Unless immediate changes are required, suggestions will be discussed at the annual review of the Policy.

3.5 Policy Awareness

The Health & Safety Manager will send an electronic copy of this policy to each new member joining the Company and keep the current edition readily available on the Company's website. Following each review, the Health & Safety Manager will send the URL of the updated Security Policy to all Heads of Managers. All members are expected to be familiar with, and to comply with, the Security Policy at all times. The Health & Safety Manager will, in the first instance, be responsible for interpretation and clarification of the Security Policy. Members requiring education about any aspects of this Policy should discuss their needs with the Health & Safety Manager.

3.6 Applicability and Enforcement

This Policy applies to all members of the Company and those who use its facilities and information. Compliance to the Policy will be part of the contract of employment.

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

B. Ihenachor
Managing Director
February 2003