Information security policy

Awareness and training

Version	Date	Who	What
DRAFT	March 2023	Gary Hinson	Template prepared for SecAware

Policy summary

This policy specifies an information security awareness and training program to inform and motivate all workers regarding their information risk, security, privacy and related obligations.

Applicability

This policy applies throughout the organisation as part of the corporate governance framework. It applies regardless of whether or not workers use the computer systems and networks, since workers are expected to protect all forms of information asset including computer data, written materials/paperwork and intangible forms of knowledge and experience. This policy also applies to third-party employees working for the organisation whether they are explicitly bound (*e.g.* by contractual terms and conditions) or implicitly bound (*e.g.* by generally held standards of ethics and acceptable behaviour) to uphold our information security policies.

Policy detail

Background

Technical *IT security* (cybersecurity) controls are a vital part of our information security framework but are not in themselves sufficient to secure all our information assets. Effective information security also requires the awareness and proactive support of all workers, supplementing and making full use of the technical security controls. This is obvious in the case of social engineering attacks and frauds, for example, which directly target vulnerable humans rather than IT systems.

Lacking adequate information security awareness, workers are less likely to recognise or react appropriately to information security threats and incidents and are more likely to place valuable information in danger through ignorance and carelessness.

Whereas 'awareness' implies general vigilance and a basic level of understanding about a broad range of information security matters, 'training' implies more narrowly-focused and detailed attention to one or more specific topics. Training tends to be delivered through classroom or online courses, while awareness tends to be delivered by multiple communications methods such as seminars, case studies, written briefing and reference materials (for self-motivated study), posters, briefings and conversations. Awareness provides the foundation level of knowledge and understanding for training to build upon. In other words, security awareness and training are complementary approaches.

Policy axiom (guiding principle)

In order to protect valuable information, all workers must be informed about relevant, current information risk and security matters, and motivated to fulfil their obligations.

Detailed policy requirements

1. An information security awareness program should ensure that all workers achieve and maintain at least a basic level of understanding of information security matters, such as general obligations under various information security policies, standards, procedures, guidelines, laws, regulations, contractual terms plus generally held standards of ethics and acceptable behaviour.
2. Additional training is appropriate for workers with specific roles and responsibilities in information security that are not satisfied by basic security awareness, for example Information Risk and Security Management, Security Administration, Physical/Site Security and IT/Network Operations personnel. Such training requirements must be identified in workers' personal training plans and funded accordingly. The particular training requirements will reflect workers' relevant prior experience, training and/or professional qualifications, as well as anticipated job needs.
3. Security awareness and training activities should commence as soon as practicable after workers join the organisation, for instance through attending information security induction/orientation sessions. The awareness activities should proceed on a continuous, rolling basis thereafter in order to maintain a reasonably consistent level of awareness of current issues and challenges in this area.
4. Where necessary and practicable, security awareness and training materials should suit their intended audiences in terms of their styles, formats, complexity, technical content *etc*. For example, some people prefer to read written descriptions and instructions while others prefer to be shown things or have them demonstrated. Some like to read words, others prefer diagrams and pictures. Non-technical workers are unlikely to understand or appreciate highly technical awareness content, while their technical colleagues may well need the full details in order to understand exactly what they are being asked to do. Everyone needs to know why information security is so important, but the motivators may be different for workers concerned only about their own personal situations or managers with broader responsibilities to the organisation and their staff.
5. Information Security's intranet site (the *Security Zone*) is the focal point for security awareness, providing information and guidance on a wide variety of information security matters. It is the *definitive* source of current information security policies, standards, procedures and guidelines. However, workers with limited intranet access must also be kept suitably informed by other means such as seminars, briefings and courses.
6. A range of measures must be undertaken to ensure compliance with information security-related legal, regulatory and contractual obligations, and conformity with other requirements such as corporate policies and applicable standards. While the details vary according to the specific nature of those obligations and requirement including the risks associated with non-compliance/non-conformity, management anticipates a mixture of routine, periodic and *ad hoc* compliance and conformity activities such as management oversight, reviews and audits,

which may include checking workers' uptake of security awareness and training opportunities, awareness test results and other metrics.

Responsibilities and accountabilities

- **Information Security** is responsible for developing and maintaining a comprehensive suite of information security policies (including this one), standards, procedures and guidelines that are to be mandated and/or endorsed by management where applicable. Working in conjunction with other corporate functions and **Information Owners**, it is also responsible for running suitable awareness, training and educational activities to raise awareness and aide understanding of workers' responsibilities identified in applicable policies, laws, regulations, contracts *etc*.

- The **Chief Information Security Officer/Information Security Manager** is accountable for running an effective information security awareness and training program that informs and motivates workers to help protect the organisation's information assets, and third-party information (including personal data) in our care.

- **Help Desk** is responsible for helping workers on basic information risk, security, privacy and related matters, liaising with experts from functions such as Information Security, Physical/Site Security, IT, Human Resources, Risk Management, Legal/Compliance where necessary.

- **Managers** are responsible for ensuring that their staff and other workers within their remit participate in the information security awareness, training and educational activities where appropriate.

- **Workers** are personally accountable for compliance with applicable legal, regulatory and contractual obligations, and conformity with policies at all times.

- **Internal Audit** is authorised to assess conformity with this and other corporate policies at any time.

Further information

For general advice on information risk and security matters, speak to your manager, contact the Help Desk or browse the intranet *Security Zone*. Contact Information Security or Human Resources for more specific advice and assistance.

Copyright and disclaimer

This is a generic example policy, a template. It is not intended to suit all organisations and circumstances. It is merely guidance. Please refer to the ISO/IEC 27000 standards and other definitive sources including qualified legal counsel in preparing your own security policies.