Information security policy

Change and configuration management

Version	Date	Who	What
DRAFT	October 2022	Gary Hinson	Template prepared for SecAware

Policy summary

This policy lays out cost-effective information security arrangements for managing and controlling changes to business processes and/or the supporting IT systems, networks, configurations *etc.*, in order to minimise the organisation's information risks.

Applicability

This policy applies throughout the organisation as part of the corporate governance framework. It is particularly relevant to changes affecting the main corporate IT systems/networks and critical business processes. It also applies to changes on less important IT systems/networks and processes including those shared within workgroups or developed and used by individuals. 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

Virtually all changes are associated with risks to varying extents, while sometimes failing to change or delaying changes can also be risky (*e.g*. not responding to new compliance obligations or emerging information security threats). Badly managed or uncontrolled changes, especially those involving major corporate IT systems/networks and critical business processes, can cause disruption, lead to system/network/process/service failures, introduce information security vulnerabilities or expose the organisation to different threats, and increase costs. Unwise or mismanaged changes may threaten the organisation's efficiency, effectiveness, compliance and ultimately its survival.

Policy axioms (guiding principles)

A. Changes to management systems, business processes and the associated IT systems, networks, applications *etc*. must be competently planned, managed, directed and controlled to minimise information risks.

B. The extent and nature of management control should reflect the degree of risk inherent in the changes.

C. Changes must fulfil any compliance obligations imposed by the laws, regulations and contractual obligations, and conform with applicable policies and standards in effect at the time of implementation.

Detailed policy requirements

1. Anyone making changes to business processes and/or the associated IT systems/networks must follow the organisation's change management and control processes, including:
   - Analysing and documenting the proposed changes;
   - Assessing and treating the associated risks, particularly information risk;
   - Gaining management authorisation for the release, including approval by the relevant Information Owners, where applicable;
   - Managing and controlling system/cloud configurations and settings, software versions, users and support documentation *etc*.
2. Risks associated with changes to systems/networks and processes must be assessed as part of the management process. If they are unacceptable to the Information Owners whose information is involved in, or likely to be impacted by, the changes, the risks must be treated, normally through assurance and resilience controls such as:
   - Standard 'template' installations with secure configuration settings (*e.g*. no unnecessary privileged accounts and utilities, standardised security logging and alarms);
   - Pre-release (production acceptance) testing;
   - Post-release (verification) testing;
   - Backups and back-out arrangements, plus business continuity arrangements to minimise adverse business impacts if a change implementation should fail.

   The actual requirements depend on the risks arising from a given situation. Occasionally the risks may be so severe that changes may be halted or delayed pending redesign, additional testing or other approaches (risk avoidance).
3. Other valuable information is also subject to change from time to time, for example new business relationships and new workers. The corresponding information risks should be managed in the same way.
4. In order to comply with our obligations under various laws, regulations and contracts, changes may be imposed upon us, forbidden, or modified. For example, changes that impinge upon personal information must not make us noncompliant with the relevant privacy laws and regulations. Compliance may therefore be another factor to be considered by the Information Owners, taking advice from the relevant professionals.
5. We must also conform to information risk and security objectives, policies, directives *etc*. formally expressed by management, or seek authorised exemptions.

Responsibilities

- **Information Security** is responsible for maintaining this policy and advising generally on information security controls. Working in conjunction with other corporate functions, it is also responsible for running educational activities to raise awareness and understanding of the obligations identified in this policy.
- **IT** is responsible for following the IT change management process for changes to all corporate IT systems/networks, including the process controls noted in this policy.
- **Information Owners** are personally accountable for the protection and legitimate exploitation of 'their' information. They have a direct interest in ensuring that changes and configurations are properly managed and controlled in order to minimise unacceptable and unnecessary risks.
- **Risk Management** and **Legal/Compliance** are responsible for providing suitable guidance and advice to those managing and performing changes.
- **Help Desk**, in conjunction with specialists from IT, Risk Management, Information Security, Risk Management *etc*., is responsible for advising IT users and managers on techniques to minimise the risks associated with IT changes.
- **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 compliance with this and other corporate policies at any time.

Further information

For help with this policy, please contact the Help Desk or browse the intranet *Security Zone*. For more specific advice, contact Information Security or IT.