INFORMATION SECURITY POLICY

Label: Global, Public

Accelerating success.

Introduction

This document defines the Information Security Policy (ISP) and how an Information Security Management System (ISMS) will, be managed, measured, reported on, and developed within Colliers International.

The ISMS program aims to:

- Protect Colliers' intellectual property client information and Colliers critical systems from cyber-attacks.
- Manage and track our effectiveness on detecting, containing, and eradicating a cyber security breach.
- Enable Colliers to comply with local and international laws and regulations.
- Raise security awareness level among Colliers community members.
- Give assurance to our customers, staff, board members, suppliers, and other interested parties that their data is secure.
- Give Colliers the ability to bid for and respond to tenders for business where compliance with international standards is a requirement.
- Demonstrate to the public that Colliers International takes information security seriously.
- Improve the security of our (and our customers) information assets.
- Align information security controls with the business (and our customers) needs through regular review meetings with interested parties.

Information Security Policy

Executive Commitment

The Board of Directors and management of Colliers International, which is in the business of providing commercial real estate services on a global basis, are committed to preserving the confidentiality, integrity, and availability of all the physical and electronic information assets throughout the organization to maintain its competitive edge, cash-flow, profitability, legal, regulatory, contractual compliance, and commercial image. This will be demonstrated through this policy and the provision of appropriate resources to provide and develop the ISMS and associated controls.

Top management will also ensure that a systematic review of the performance of the program is conducted regularly to ensure that quality objectives are being met and relevant issues are identified through the audit program and management processes. Management review can take several forms including departmental and other management meetings.

Overall Responsibility

The Global Senior Director of Cybersecurity shall have overall authority and responsibility for the implementation and management of the Information Security Management System, specifically:

- The identification, documentation, and fulfilment of information security requirements
- Implementation, management, and improvement of risk management processes
- Integration of operational processes, procedures, and controls
- Compliance with statutory, regulatory, and contractual requirements
- Reporting to top management on performance and improvement

Roles and Responsibilities

The Senior Director Cybersecurity is accountable to ensure that employees and contractors understand the security roles they are fulfilling and that they have appropriate skills and competence to do so. All IT security administrators, IT security managers, and IT security analysts are responsible to educate employees and contractors about the information security program and the various policies that support the program.

Information Security Requirements

A clear definition of the requirements for information security will be agreed and maintained with the internal business and customers so that all ISMS activity is focused on the fulfilment of Colliers International's goals. The ISMS intends to be an enabling mechanism for information sharing, for electronic operations and for reducing information-related risks to acceptable levels.

Statutory, regulatory, and contractual requirements will also be documented, and input to the planning process. Specific requirements regarding the security of new or changed systems or services will be captured as part of the design stage of each project.

It is a fundamental principle of the Colliers International ISMS that the controls implemented are driven by business needs, and this will be regularly communicated to all staff through team meetings, briefing documents, and Colliers' intranet.

Colliers International's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating, and controlling information-related risks through the establishment and maintenance of an ISMS. The Risk Assessment, Statement of Applicability and Risk Treatment Plan identify how information-related risks are managed. Click here to enter text.The global and local IT security personnel are responsible for the management and maintenance of the risk treatment plans. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

Framework for Setting Objectives

Business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy.

Colliers International aims to achieve specific and defined information security objectives, which are developed in accordance with the business objectives, the context of the organization, the results of risk assessments and the risk treatment plan.

Application of Information Security Policy

All staff of Colliers International and sub-contractors shall comply with this policy and with the ISMS that implements this policy. All staff, and sub-contractors, will receive appropriate training. The consequences of breaching the information security policy are set out in the Organization's disciplinary policy and in contracts and agreements with third parties.

Continual Improvement of the ISMS

The ISMS is subject to continuous, systematic review and improvement.

Colliers International policy regarding continual improvement is to:

- Continually improve the effectiveness of the ISMS.
- Review to respond to any changes in the risk assessment or risk treatment plans and at least annually.
- Enhance current processes to bring them into line with good practice as defined within ISO/IEC 27001 and related standards.
- Achieve ISO/IEC 27001 certification readiness and maintain the program on an ongoing basis.
- Increase the level of proactivity (and the stakeholder perception of proactivity) regarding information security.
- Make information security processes and controls more measurable to provide a sound basis for informed decisions.
- Review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data.
- Obtain ideas for improvement via regular meetings and other forms of communication with interested parties, including cloud service customers.
- Review ideas for improvement at regular management meetings to priorities and assess timescales and benefits.

Ideas for improvements may be obtained from any source, including employees, customers, suppliers, IT staff, risk assessments, and service reports. Once identified they will be recorded and evaluated as part of management reviews.

The following criteria will be used in the assessment of improvement proposals:

- Cost
- Business Benefit
- Risk
- Implementation timescale
- Resource requirement
- Strategic Alignment to adding business value and business objectives

If accepted, the improvement proposal will be prioritized to allow more effective planning.

Information Security Policy Areas

Colliers International defines the ISMS in a wide variety of information security-related control objectives as described in Annex A of the ISO/IEC 27001:2013 standard.

Each control objective is defined and agreed by one or more people with competence in the relevant area and once formally approved, is communicated to an appropriate audience, both within and external to the organization.

In this policy, 'information security' is defined as:

Preserving

This means that management, all full time or part-time staff, sub-contractors, project consultants and any external parties have and will be made aware of their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches and to act in accordance with the requirements of the ISMS. All staff will receive information security awareness training, and more specialized staff will receive appropriately specialized information security training.

The availability,

This means that information and associated assets should be accessible to authorized users when required and, therefore, physically secure. The business systems including its networks, infrastructure, websites, and business applications must be resilient and Colliers must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems, and information. There must be appropriate business continuity plans.

Confidentiality

This involves ensuring that information is only accessible to those authorized to access it and, therefore, to preventing both deliberate and accidental unauthorized access to Colliers International's information and its systems, including its networks, infrastructure, websites, and business systems.

and Integrity

This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial, or complete, destruction, or unauthorized modification of either physical assets or electronic data. There must be appropriate contingency and data backup plans and security incident reporting. Colliers must comply with all relevant data-related legislation in those jurisdictions within which it operates.

of the physical (assets)

The physical assets of Colliers including, but not limited to, computer hardware, data cabling, telephone systems, filing systems, and physical data files.

and information assets

The information assets include information printed or written on paper, transmitted by post, or shown in films, as well as data stored electronically on servers, website(s), extranet(s), intranet(s), PCs, laptops, mobile phones, and PDAs, as well as on CD ROMs, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context, 'data' also includes the sets of instructions that tell the system(s) how to manipulate information (i.e., the software: operating systems, applications, utilities, etc).

Of Colliers International.

Colliers International (Colliers) and such partners that are part of our integrated network have signed up to our security policy and have accepted our ISMS.

The ISMS is the Information Security Management System, of which this policy, the Information Security Manual ('the Manual') and other supporting and related documentation is a part, and which has been designed in accordance with the specification contained in ISO27001:2013.

A **CYBER SECURITY INCIDENT** is an occurrence that involves any unauthorized access to Colliers internal IT systems or Colliers provided IT cloud services.

A **CYBER SECURITY DATA BREACH** is a cyber security incident when private, confidential or highly confidential (i.e., Restricted) Colliers' data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so.

Approach to Managing Risk

Risk management will take place at several levels within the ISMS, including:

- Management planning – risks to the achievement of information security objectives will be assessed and reviewed regularly.
- Information security and IT service continuity risk assessments.
- Assessment of the risk of changes via the change management process.
- As part of major projects to achieve business change, e.g., new computer systems and services.

High-level risk assessments will be reviewed on an annual basis or upon significant change to the business or service provision.

A risk assessment process will be used, which is in line with the requirements and recommendations of ISO/IEC 27001, the International Standard for Information Security.

From this analysis, a risk assessment report will be generated, followed by a risk treatment plan in which appropriate controls will be selected from the reference list in Annex A of the ISO/IEC 27001 standard.

People Services (HR) Security Management

Colliers will ensure that all staff involved in information security are competent based on appropriate education, training, skills, and experience.

The skills required will be determined and reviewed regularly, together with an assessment of existing skill levels within Colliers International. Training needs will be identified, and a plan maintained to ensure that the necessary competencies are in place.

Training, education, and other relevant records will be kept by the appropriate IT Manager of the individual contributor to document individual skill levels attained.

Auditing and Review

Once in place, it is vital that regular reviews assess how well information security processes and procedures are being followed. This will happen at three levels:

1. Structured regular management review of conformity to policies and procedures.
2. Internal audit reviews against the ISO/IEC 27001 standard (and accompanying codes of practice) by the Colliers International Internal Audit Team.
3. Where applicable, external audit against a Registered Certification Body's standard to gain and maintain certification.

Documentation Structure and Policy

All information security policies and plans must be documented.

Control of Records

The keeping of records is a fundamental part of the ISMS. Records are essential information resources and represent evidence that processes are being carried out effectively.

Non-Compliance

Violations of this policy will be treated like other allegations of wrongdoing at Colliers International. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

- Disciplinary action according to applicable at Colliers International policies.
- Termination of employment; and/or
- Legal action according to applicable laws and contractual agreements

Document Owner and Approval

The *Senior Director, Cybersecurity,* is the owner of this document and is responsible for ensuring that this policy document is reviewed annually.

A current version of this document is available to all members of staff on the corporate intranet. It does not contain confidential information and can be released to relevant external parties.

This policy was approved by the Global Sr. Director of Cyber Security and is issued on a version-controlled basis under his signature.

Signature:

Date:

2 August 2022

Dave Davies

Global Sr. Director of Cyber Security