

Information Security Policy

ISO Control Ref.: 5.2

Document Version 6.0

Contact

Phone: 0800 044 5009
Email: hello@kocho.co.uk
Website: kocho.co.uk



Confidentiality

This document is classified as CORPORATE OFFICIAL and can be distributed outside of Kocho. This document and its contents are provided AS IS without warranty of any kind. All trademarks are the property of their respective companies. The names of actual companies and products mentioned may be the trademarks of their respective owners.

Identification

File Name	Owner
Information Security Policy	Information Security Manager

Preparation & version tracking

Version	Title	Date	Action/comment
0.1	Information Security Manager	08/06/2021	Previously separate ThirdSpace and TiG InfoSec Policies combined into new corporate template
1.0	Information Security Manager	25/06/2021	Issue 1 approved by Group DPO
2.0	Information Security Manager	05/10/2021	Annual review: Minor edits to clarify titles of documents and roles within the organisation
2.1	Information Security Manager	21/04/2022	Re-templated into Kocho template
3.0	Head of Compliance	07/10/2022	Annual review: Minor textual edits for clarity
3.1	Head of Compliance	07/12/2022	Document classification updated
4.0	Head of Compliance	19/10/2023	Annual review: Contact details updated
5.0	Compliance Officer	10/10/2024	Annual review: No updates.
6.0	Information Security Officer	17/10/2025	Annual review: No updates.

Reviewers/Authorisers

Title	Reviewer/Authoriser	Date	Date of Next Review
Group DPO	Authoriser	17/10/2025	October 2026



Contents

1	Purpose of Document.....	4
2	Management Commitment.....	4
3	Responsibilities	5
4	Review	5
5	Definitions.....	6



1 Purpose of Document

Information is critical in ensuring the continued and effective operation of both Kocho and its clients. It is therefore essential that Kocho and client information/data is afforded the appropriate and proportionate level of protection in accordance with legislative and regulatory requirements, and security good practice.

The purpose of this Information Security Policy is to clearly define and communicate our information security obligations from the perspective of both the organisation and individually as an employee, contractor or third party, ensuring that information is appropriately protected. In this Policy, 'information security' is defined as:

Preserving the Confidentiality, Integrity and Availability of the physical assets and information assets of Kocho.

2 Management Commitment

The Board of Directors and management of Kocho are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout the organisation in order to preserve its competitive edge; cash-flow; profitability; legal, regulatory and contractual compliance and commercial image. Information and information security requirements will continue to be aligned with Kocho's goals and the Information Security Management System (ISMS) is intended to be an enabling mechanism for information sharing, for electronic operations and for reducing information-related risks to acceptable levels.

An annual cycle will be used for the setting of objectives for information security. This will ensure that adequate funding is obtained for the improvement activities identified. These objectives will be based upon a clear understanding of the business requirements, captured during management reviews with stakeholders. Objectives will be documented for the relevant financial year, together with details of how they will be achieved. These will be reviewed on a periodic basis to ensure that they remain valid.

Kocho's current strategic business plan and risk management framework provides the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an ISMS. The Statement of Applicability, Risk Register and Risk Assessment & Treatment Plan identify how information-related risks are controlled. The Information Security Manager (ISM) is responsible for the management and maintenance of the Risk Register. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

In particular, 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.



3 Responsibilities

It is the responsibility of all employees and certain external parties identified in the ISMS to:

- Protect information or data in accordance with this and all Kocho policies, data protection legislation/regulations and security good practice;
- Comply with this Policy and with the ISMS that implements this Policy.

All employees, and certain external parties, will receive appropriate training. The consequences of breaching this Information Security Policy are set out in Kocho's disciplinary policy and in contracts and agreements with third parties.

All incidents, near misses and observations relating to information/data must be reported as soon as identified to the Group Data Protection Officer (DPO). The DPO is responsible for ensuring that all events relating to a suspected incident are investigated quickly and thoroughly to enable any confirmed security breach to be escalated to the Board Level Sponsor and relevant clients, and for notifying the UK Information Commissioner's Office (ICO) within 72 hours.

Primary Contact	Secondary / Escalation Contact
Group DPO	Board Level Sponsor
Jacques Fourie – Global Operations Director and Group DPO Email: jacques.fourie@kocho.co.uk	George Georgiou – Chief Operations Officer Email: george.georgiou@kocho.co.uk

4 Review

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

Kocho has established an Information Security Committee, chaired by the Chief Operations Officer (COO) and comprising the Group DPO, Head of Governance and Sustainability (acting in the role of Information Security Manager) and other executives or specialists to support the ISMS framework and periodically review the Information Security Policy.

Kocho is committed to ongoing certification to the ISO 27001 standard.

This Policy is reviewed at least annually and to respond to any changes in the Risk Register.



5 Definitions

Term	Meaning
Preserving	This means that management, all full time or part time employees, 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 (in line with the policy and procedures identified in the ISMS) and to act in accordance with the requirements of the ISMS. All employees will receive information security awareness training and more specialised staff will receive appropriately specialised information security training.
Confidentiality	This involves ensuring that information is only accessible to those authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to Kocho's information and proprietary knowledge and its systems including its network, website, and e-commerce systems.
Integrity	This involves safeguarding the accuracy and completeness of information and processing methods, and preventing deliberate or accidental, partial or complete, destruction or unauthorised modification of either physical assets or electronic data. There must be appropriate contingency including for network, website, and data backup plans and security incident reporting. Kocho must comply with all relevant data-related legislation in those jurisdictions within which it operates.
Availability	This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be resilient and Kocho 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.
Physical Assets	The physical assets of Kocho including, but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.
Information Assets	<p>The information assets include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, websites, intranet, PCs, laptops, mobile phones, as well as on CD ROMs, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means.</p> <p>In this context, 'data' also includes the sets of instructions that tell the systems how to manipulate information (i.e. software, operating systems, applications, utilities, etc.)</p>
Information Security Management System (ISMS)	<p>The Information Security Management System, of which this Policy and other supporting and related documentation is a part, and which has been designed in accordance with the specification contained in ISO 27001.</p> <p>Kocho and such partners that are part of our integrated network have signed up to our Information Security Policy and have accepted our ISMS.</p>
Security Breach	An incident or activity that causes, or may cause, a break down in the confidentiality, integrity or availability of the physical or electronic information assets of Kocho.

About Kocho

At Kocho, we believe greatness lies in everyone.

That's why we exist, to help ambitious companies realise their potential.

By combining the power of Microsoft cloud technology with world-class identity, cyber security and our team of talented people, we take our clients on a journey of secure cloud transformation.

And we're with you every step of the way. Because the path to greatness isn't walked alone. We help you adopt and embrace the right technology solutions at the right time.

The result? Sustainable and secure growth that amplifies your business success.

Kocho. Become Greater.

Kocho 

 Microsoft
Solutions partner

Think
greater.




Better
together.



Do what's
right.



 hello@kocho.co.uk

 0800 044 5009

