The Copper Mark

Information Management Policy

February 2024

The Copper Mark, a Private Limited Company by guarantee, Company Number 12370476, registered at 10 North Place, Cheltenham GL50 4DW, UK.

Revision Date:	Publication Date:	Organization:
8th January 2024	12th March 2024	The Copper Mark
Title:	**Version number:**	**Type:**
The Copper Mark Information Management Policy	1	Internal

Table of Contents

Introduction and Purpose

The Copper Mark is the leading assurance framework that promotes responsible practices across the copper, molybdenum, nickel and zinc value chains. The Copper Mark works with companies and organizations throughout these metals' value chains to enable them to better understand and meet the increasing demands for independently verified responsible practices, and to contribute positively to sustainable development.

Information Management is key to effective information governance, risk control, and ensuring compliance. This policy sets out a high-level view of how information is managed and governed within The Copper Mark and provides links to more detailed guidance where appropriate.

Scope

This policy relates to all Copper Mark staff and is applicable to information and records collected, processed, and stored for the purposes of the organization.

The policy also covers all applications used to create, manage or store information and records, including records management systems, email, websites, social media applications, databases, and financial management systems.

Policy Summary

The Copper Mark recognizes information assets as valuable resources to help it meet its vision and is committed to achieving appropriate and ongoing management of these assets to advance the organization's strategic and near-term goals and reputation.

The organization will plan for the future of its information assets, its staff capabilities, and invest to protect the information contained in those assets.

Legislative and Regulatory Environment

The legal and regulatory environment that The Copper Mark works in provides a baseline for standards in its information management. The main legal data protection requirements are those of the General Data Protection Requirements as enshrined in law via the UK Data Protection Act 2018 (DPA 2018).

Not only are these requirements vital for The Copper Mark's compliance position but they also provide a framework for effective information management, ensuring that we have the right information at the right time to make the right decisions and pursue The Copper Mark vision.

All staff must take steps to protect personal information according to the Data Protection Framework, and this includes information stored in cloud-hosted environments such as Office365.

Further information:

- Appendix A: Data Protection Framework
- Appendix B: Information Security Framework
- Appendix C: ISEAL Data Maturity Requirements

Reputation and Trust

Organizations that exist to provide assurance have an existential interest in being trusted themselves and this is an important part of the value they provide, both to clients and to the wider public.

The Copper Mark will seek to embody the spirit of best practice alongside compliance with regulations in its information management practices and embed a culture of continuous improvement in information management, governance, and security. The Copper Mark is subject to membership requirements of ISEAL, which specify data maturity requirements across the topics of data culture, data structure and data use;

Although compliance with international standards (such as ISO27001) is not a requirement of The Copper Mark's business, these standards can be used to assess and plan improvements to information management, governance and security across the organization.

Further information:

- Appendix D: ISO27001 compliance outline

Roles and Responsibilities in Information Management

Clearly defined roles and responsibilities provide the mechanism to enable data management to be seamlessly integrated to the day-to-day operations of the organization. It is the responsibility of all Copper Mark staff to ensure that information is accurate, reliable, ordered, complete, up to date and accessible to enable the correct operation of the organization and make informed decisions.

The following roles and responsibilities are required for effective information management:

Role	Responsibilities
Executive owner	• Acts as the executive sponsor for the information management program. • Establishes the information management program's vision, goals, and objectives. • Ensures the information management program receives adequate resources. • Monitors compliance with the organization's information management policies.
Policy owner	• Owns the information management policy. • Verifies that the information management policy is followed and implemented.

	• Reviews the information management policy annually to ensure that it is up to date with the latest industry and organizational requirements. • Responsible for data analysis and reporting.
Records manager	• Defines information management procedures. • Performs regularly scheduled records disposition review. • Creates and delivers information management policy training to staff. • Assists with report creation and data extraction. • Supports others in daily use of data systems.
Record Creators and Users	• Properly store all documents electronically in the corporate content repository • Identify document contents through defined naming and metadata conventions • Send reference links to documents internally and not the actual document via email and chat, to limit proliferation of document copies • Adhere to security practices and confidentiality expectations for information and data. • Raise concerns about security risks or system malfunctions.

Information Assets

The Copper Mark utilizes a modern IT infrastructure based around Microsoft Office 365, which should be accessed securely only from devices managed by the organization.

Devices in use comprise:

- Laptops
- Smartphones

The organization runs remotely and so all files are stored and accessed in the Office 365 cloud. In some cases, files are held locally by specific staff members, but these must also be securely backed up.

There are a small number of other cloud-based systems in use, including EthicsPoint, and Outlook.

These systems are detailed in the Information Asset Register.

Managing risks to information assets

All information collected, processed or stored by the organization will have a corresponding entry in the Information Asset Register. This document contains all the necessary information to manage compliance and risk around the organization's information.

The records of the day-to-day operations of The Copper Mark are maintained in the organization's Office 365 instance. Documents can also be maintained on company laptops and cellphones but must be automatically backed up to this cloud.

An Information Risk Register is maintained alongside the Information Asset Register and Record of Processing Activities. This register informs and prioritizes the actions needed to protect information assets.

Storage, retention, and disposal of information

Keeping information secure and accessible is vital to help us measure our progress towards the Copper Mark vision - and report on it as well. We also need to keep records to comply with regulatory requirements, to protect legal and other rights and interests, and to be able to build better systems based on continuous improvement.

The types of information we collect and why we collect it

Beyond personal information, covered in the Privacy Notice, we collect information relevant to fulfill the activities of the assurance process and its related processes. We manage this information in accordance with its sensitivity.

Examples include but are not limited to:

- Figures for provider company revenue, turnover and accounts
- Assessment findings, especially when these are reflective of issues with the provider's operational standards or working conditions.
- Due diligence reports where providers are found to have past or pending legal challenges or other adverse media.

This information can be categorized into three sets:

- Activity – assurance management pipeline
- Contacts – partners and individual sites
- Reference – reports and research

Confidential data is found in all the three sets of core data, and must be stored, processed, retained and disposed of in such a way as to ensure confidentiality, integrity and availability. This information and its confidentiality level are contained in the Information asset register.

How our data is stored

The Copper Mark utilizes Office365 for its core infrastructure, and the use of SharePoint within this solution is the default storage location for all business documents at most levels of sensitivity.

Exceptions to this are:

- Press releases and other media content. These are generally posted on the appropriate channel, for example Dropbox; X/Twitter; LinkedIn; or Constant Contact.
- Training materials. These also reside on YouTube and The Copper Mark website.
- Partner and Participant Communications. These will appear on the preferred channels of our partners, for example WhatsApp, WeChat Email or iMessage.
- Meeting materials, shared with third parties using Dropbox.
- Confidential whistleblowing reporting. This is recorded on EthicsPoint where appropriate.
- Employment records held privately by senior leadership.

Other exceptions may be created by senior leadership and recorded on the Information Asset Register as needed.

The procedure to this policy provides guidance to staff to choose the right place to store information, how to use the naming convention and how to categorize it in accordance with confidentiality level.

Automated backups are maintained on cloud-to-cloud solutions via a third-party provider.

Information and data are shared via authorized channels only, email or cloud sharing, to third parties that commit to extend the protections to such data.

Information and data are stored while needed for the operation of the organization or as legally required, whichever is longer.

At the end of the data lifecycle, we dispose of this information by first transferring it to an archive and scheduling deletion.

Disposition decisions must be recorded and approved by the respective Information Asset Owner.

Communication and Training

This policy is supported by training for all staff on an annual basis, on the content of the policy and related procedure. Staff will be required to read the policy, both during onboarding and following revisions to the policy.

Monitoring and Review

Monitoring the implementation of the policy and its supporting procedure will be undertaken on an annual basis. Monitoring and compliance will be supported by external audits where appropriate.

Internal and external audit results should be integrated into the annual review of the policy and procedure and action plans followed to closure.

Resources

- The Copper Mark - Privacy Notice
- Data Management Procedure
- Information Asset Register / Record of Processing Activities / Information Risk Register
- Data Protection Impact Assessment template
- Personal Information Security Policy (see Appendix E)

Key Contacts:

Hillary Amster, COO, hillary.amster@coppermark.org

Michèle Brülhart, Executive Director, michele.brulhart@coppermark.org

Appendix A: Data Protection Framework

Our approach is guided by the United Kingdom General Data Protection Regulation contained in the Data Protection Act 2018 (DPA 2018) and its key principles, which are building blocks for data protection practice. These key principles are:

Principle	Explanation
Lawfulness, fairness, and transparency	There must be valid legal grounds for collecting and processing personal data; data must be processed in accordance with the law; data must not be processed in a way that is detrimental, misleading or unexpected; and the ways in which data is processed must be clearly communicated to data subjects.
Purpose limitation	The purpose for collecting personal data must be clearly stated, recorded and communicated; this purpose can only be changed or extended if it is compatible with the original purpose, or if consent is obtained
Data Minimization	The data being processed must be adequate, relevant, and limited to what is necessary for the purpose specified.
Accuracy	All steps must be taken to ensure that personal data is accurate and up to date, and processes must exist to correct inaccurate or outdated information.√
Storage Limitation	Data must not be kept for longer than needed. Retention periods must be documented and justified. Data held must be periodically reviewed to ensure it is still needed. There must be a process to fairly consider challenges to your need to keep an individual's data.
Integrity and Confidentiality	You must ensure that you have appropriate security measures in place to protect the personal data you hold.
Accountability principle	Take responsibility for what you do with personal data and how you comply with the other principles. You must have appropriate measures and records in place to be able to demonstrate your compliance.

Further information: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/

The personal data protection practices of The Copper Mark, to ensure meeting its obligations under the UK GDPR, are communicated to stakeholders in the organization's Privacy Notice, which applies to all the information processed by The Copper Mark through its different processes.

The Privacy Notice, publicly available on the website: coppermark.org, describes whose personal information we use, what information we collect, the sources of such information, how is this information used and shared, how is this information kept safe and how long it is kept. Instructions are made available on the rights of the individuals that provide personal data, including instructions on how to contact The Copper Mark to exercise those rights, and how to report any concerns to the supervisory authority, the Information Commissioner's Office.

The Record of Processing Activities (RoPA) is a derivative of the Information Asset Register that covers those information assets that contain personal information and includes the legal basis on which that information is processed. This information then populates the relevant areas of the Privacy Notice.

In the rare cases that information processed is both personally identifying and sensitive, a Data Protection Impact Assessment must be carried out. A template for this is provided.

Appendix B: Information Security Framework

To ensure the security of electronic information and the physical media used by the Copper Mark staff, the following framework is in place to manage the risk of information loss or data breach. The controls outlined are based on ISO27001 (Information Security Management) standard, although The Copper Mark is not required to be accredited to the standard. The same is true of UK Government backed standards such as Cyber Essentials.

Cybersecurity protections cover all aspects from access to information, email standards, security access levels based on confidentiality, credentials, device management, software updates, secure networks, implement information protection practices and procedures for reporting privacy breaches or data misuse.

Information governance practices should be carefully followed to mitigate risk to information; such risks include data breach, data leak, operational disruption, malware infections, and phishing attacks, among others.

Organization of Information Security

Each information asset in the Information Asset Register is assigned a dedicated owner who is accountable for the security of the information it contains.

At an enterprise level, this accountability is owned by a board member with the role of Senior Information Risk Owner. This role is currently occupied by ____.

Responsibility for securing individual systems can be delegated to those with specific skills or third-party providers, but accountability remains with the information asset owner.

Human Resources

The effectiveness of Information Security policies rests with their implementation by staff members. To help with this a Personal Information Security Policy (Appendix E) is provided for each member of staff, providing guidance about the secure use of information whilst carrying out their role.

Staff are required to read and commit to the details of the policy during employee induction.

Should staff change jobs internally, their security access may be required to change accordingly.

When staff leave the organization, their access must immediately be removed.

Physical and Environmental Security

The Copper Mark is a distributed organization that operates without fixed premises. Because of this it is vital that the machines and locations that staff work from are secured as far as possible, with the use of TCM-managed devices throughout. Company computers running Windows OS must have anti-virus software; all devices should have encrypted hard disc drives as well as installing software updates as soon as they become available.

Workstation and home office security questionnaires (Appendix F) should be completed by all staff.

Access Control

The use of access credentials to identify and authenticate users that meet security requirements is a key target for security controls, including password strength, use of password managers, password expiration policy, and disabling old credentials. The accountability for access control to each information asset rests with the respective Information Asset Owner, but in practice access to all The Copper Mark information assets is controlled by Microsoft Office365 Administrator console.

Confidentiality levels are based on data sensitivity and user functions or “need to know”. These levels are “Public user”, “Internal information”, “Restricted information”, and “Confidential Information”. The Copper Mark documents are labeled in accordance with confidentiality; simultaneously, accounts are configured to enable access to the respective confidentiality level. Automated auto-tagging is enabled in the cloud storage solution.

Confidentiality levels are assigned in accordance with the information asset register.

Systems development, acquisition, and maintenance

Security will be considered when developing or otherwise commissioning new systems for the company and preference will be given to systems suppliers who can demonstrate a clear commitment to information security (for example by holding a relevant ISO27001 or Cyber Essentials Plus certification) and/or follow secure development practices such as OWASP.

Incident Management

The Copper Mark staff are to report any privacy breach, data misuse, system malfunction (hardware or software) or any other security risk identified, related to the content of this policy and its procedure. This process allows the identification of areas of opportunity and their timely remediation.

Clear information will be disseminated to staff in the Personal Information Security Policy on what type of issues to identify and how to report it. Once an incident has been reported, the steps to carry out an investigation The Copper Mark staff is to report any privacy breach, data misuse, system malfunction (hardware or software) or any other security risk identified, related to the content of this policy and its procedure. This process allows the identification of areas of opportunity and their timely remediation.

The member of staff acting as the Senior Information Risk Owner is responsible for determining the steps required to investigate incidents and carry out a remediation plan. All incidents must be logged, and some may need to be reported to those affected, or the Information Commissioner based on their own guidance:

https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/

Please refer to the Information Risk Register for details of mitigating actions and associated contingency plans. Should a risk manifest which is not on the register, an entry should be added to it: information security is a constantly evolving practice.

Business Continuity

The Copper Mark plans for the non-availability of Information Assets. In most cases, this is as simple as having backups in place – these are automatically created by a 3rd party provider. The Senior Information Risk Owner is accountable for ensuring that the organization can continue, within reason, should some or all its information assets become unavailable. These plans are documented in the Information Risk Register.

Appendix C: ISEAL Data Maturity Guidance

Clause	Title	Additional Guidance
4.4.1	Data Sources	The scheme owner shall maintain a list of the data sources it uses to monitor risks to the integrity of the assurance system.
4.4.2	Information Management System	The scheme owner shall maintain an information management system that supports gathering, management and analysis of relevant data from internal and external sources, including compliance data from assurance providers and oversight bodies. This system can be used to inform risk management, assurance system learning, and monitoring and evaluation.
4.4.3	Data Integrity	The scheme owner shall have adequate data control protocols and sufficient capacity to ensure data consistency and integrity for the data it manages. The protocol can include criteria to assess data completeness and consistency - and can outline how the data is maintained and updated at regular intervals.
4.4.4	Data Governance	The scheme owner shall define who owns different types of assurance system data and what data is available to whom and under what conditions. This information can include who is responsible for making changes to each type of data. It can also include a publicly available data policy that summarizes the use, distribution and format by which each type of data owned by the organization is made available. A data registry can support the development of a data governance policy. When developing a data governance policy, the scheme owner may want to consider how to comply with national privacy laws related to data security and holding of personal data.
5.1.14	Records and Document Control	The scheme owner shall implement document control procedures that guide the management and storage of system documents and records.
6.1.1	Information on Performance	The scheme owner shall ensure that performance insights are provided to clients. Performance insights can be as simple as providing the client with audit reports and noting changes since the previous report. However, additional value for the client can be derived from communicating improvements over time, performance in relation to peers, or in assisting clients to understand where and how they can improve.
6.3.1	Publicly available information	The scheme owner shall ensure the following information about their assurance system and its implementation is current and publicly available:

		- Description of the structure of the assurance system including decision making (4.3.1); - Information on data ownership and availability (4.4.4); - Criteria for accepting assurance providers and clients to the scheme (6.2.1); - Application procedures for clients; - Current list of oversight bodies and assurance providers that are approved to work in the assurance scheme; - General information on fees charged to clients and applicants; - Description of the assessment methodology: type(s) of assessment employed, how clients are assessed, how often, and by whom, and the basis for decisions (evaluation framework) (5.1.2); - Policy on information provision (knowledge sharing) to clients by assurance providers (5.6.3); - Description of how stakeholders can provide input to the assurance process (6.3.2); - Description of consequences for different levels of non-conformity (5.1.10); - Summary of resolved complaints (5.1.12); - Steps taken to have confidence in the results of other schemes deemed equivalent or partially equivalent (5.3.1); - Current list of certified clients, their scope of assurance, and expiry date of their certificate (where expiry dates are used) (the list can be made available at the assurance provider level); - and Basic information about the results of assessments of both clients and assurance providers. In some cases, oversight bodies can make this information publicly available on behalf of the scheme owner. Data ownership and availability refers to what data is made available to whom and for what purposes. Scheme owners can decide what basic assessment information should be shared. Basic information can include dates, locations and scope of auditing, team composition, number and type of non-conformities, and certification status.

		Good practice is to make summary reports of assessment findings for every client publicly available. Making basic assessment information available applies to existing clients who have failed a reassessment but not to new applicants.

For the full code of good practice please visit: https://www.isealalliance.org/get-involved/resources/iseal-assurance-code-good-practice-version-20 .

Appendix D: ISO27001 compliance outline

ISO27001 is an international standard for "information security management systems" – a collection of policies, processes, organization, and technical interventions that ensure the confidentiality, integrity and accessibility of the data that underpins the successful operation of the business now and in the future.

ISO27001 does not itself contain specific technical controls (recommendations for these are specified in ISO27002) but focuses more on establishing a culture of continuous improvement across the full spectrum of data handling in the business. In this context, ISO27002 controls are implemented using a risk-based approach defined in ISO27001.

ISO27001 establishes continuous improvement across 11 separate areas (called "domains" in the literature):

- Security Policies
- Organization of Information security
- Asset Management
- Human Resources aspects
- Physical and Environmental security
- Communications and operations management
- Access Control
- Systems development, acquisition and maintenance
- Incident management
- Business Continuity
- Compliance.

There is significant philosophical and practical overlap between establishing processes and policies in these areas with other quality-based initiatives such as ISO9000 and ITIL Service Management (ITSM) frameworks.

ISO27001 uses the "Plan-Do-Check-Act" model as its basis for continuous improvement, but new ISO27001 projects always need to establish a baseline of the current situation against each domain. Following this, the first year of the process involves

- Identification of minimum required level of performance in each domain
- Gap analysis
- Improvement project
- Monitoring and evaluation.

Each following year involves a review of the findings from the previous year and a suggested program of improvements in each domain.

Having completed the first year of such a program and been assessed, the organization can be certified as being “Compliant” with the standard. After a further year of running the improvement processes the organization can then become fully “Accredited”. Evaluations must be done by a certified organization for the business to be able to market itself as being Compliant or Accredited.

As the organization grows, more resources will need to be targeted at this sort of program. Usually, the effort will be led by the information governance or compliance lead, but input from technical resources will also be required (including systems suppliers), as well as business process managers and those processing client data.

Version history

Version Number	Purpose/Change	Author	Date
1	First draft	Martin Howitt	8th January 2024