Information Security Overview - External Facing

Last Revision: June 2018

Background and Philosophy

IHS Markit is committed to safeguarding our information assets, and those of our clients, against misuse, abuse or compromise. IHS Markit adopts and fosters a risk-based approach to managing information security, with the goal of consistently implementing appropriate risk management and mitigation measures to address the threat landscape posed to IHS Markit and client data and information.

IHS Markit's business principals and corporate standards are closely aligned with our following information security objectives:

- To protect data and information assets against unauthorised access.
- To assure the confidentiality of IHS Markit and client confidential information.
- To maintain the integrity of IHS Markit data and information assets.
- To manage IHS Markit information systems in accordance with best practice.
- To comply with legal and regulatory requirements.
- To produce, maintain and test business continuity plans to protect the continuity of control and availability of IHS Markit information assets and systems.
- To ensure all IHS Markit colleagues receive Information Security Awareness Training.
- To report, investigate and escalate, where appropriate, all information security breaches, whether actual or suspected, internal or external.
- To assess and monitor the security of our supply-chain as appropriate.

Information Security Process and Framework

We undertake regular risk assessments on the threats associated with the information assets in our custody, our logical security and the third parties that provide services to us.

We manage a set of policies and documentation that reflect IHS Markit's risk appetite and are closely aligned to industry controls. The Information Security Policy Framework compliments compliance to legal, regulatory and contractual obligations.

Our Information Security Statement of Applicability defines IHS Markit's commitment to address risks identified in our risk assessments and establishes the mandates for our ongoing IHS Markit Information Security program.

Our IHS Markit Information Security Policy is applicable to all IHS Markit staff and relevant parties who have access to IHS Markit and client information assets. IHS Markit's Information Security policies, standards, guidelines, processes and technical specifications have been developed to support each of the tiers of the Information Security Control Framework.

The IHS Markit Information Security Control Framework reflects ten core control requirements. Adherence to the IHS Markit Information Security Control Framework allows IHS Markit to deploy appropriate security controls and governance to all data and supporting systems managed by IHS Markit, and to enable IHS Markit to demonstrate the safe and effective management of data and services. The ten core control requirements are:

- CA1 – Information Security Governance
- CA2 – People
- CA3 – Information
- CA4 – Systems
- CA5 – System Development and Modification
- CA6 – Device Management (IT equipment)
- CA7 – Electronic Communications
- CA8 – Customers
- CA9 – Suppliers and Partners
- CA10 – Risk and Incident Management

The selection and management of the core control requirements are aligned with relevant international standards and accreditations, including:

- ISO27001:2013 – Information Security Management System requirements
- ISO27005:2011 – Information Security Risk Management
- ISO27014:2013 – Governance of Information Security
- COBIT - Control Objectives for Information and Related Technologies for Security
- NIST SP800-100 - National Institute of Standards and Technology Information Security Handbook
- PCI-DSS - Payment Card Industry Data Security Standard
- The Sarbanes–Oxley Act 2002 – Public Company Accounting Reform and Investor Protection Act

Training: All current and new IHS Markit employees conduct and attest to completing our annual security awareness training and biannual training concerning privacy and the GDPR. Third-party representatives and contractors are vetted and trained accordingly, depending on their level of access to IHS Markit and client information assets.

Governance

Our Chief Information Security Officer (CISO) and our core internal Information security team are responsible for policy development and strategy, compliance, assurance, monitoring and incident response.

Our CISO reports to the following senior leadership team and Board of Directors:

- Executive Vice President, Chief Technology Officer
- Executive Vice President and General Counsel
- The Risk Committee of the IHS Markit Board of Directors

Our CISO attends and reports on the company's security posture, trends and threat intelligence, along with incident response, critical compliance or other strategic issues, to the Risk Committee of the IHS Markit Board of Directors on a regular basis, no less then quarterly.

Information Security Policies, Standards, Guidelines and Procedures

Below is a listing, though not exhaustive, of our policies, standards, guidelines and procedures demonstrating the breadth and scope of our IT security program. ***Note that we will not share any more detail concerning the items listed below.***

- IHS Markit Information Security Statement of Applicability
- ISO 27001 Information Security Policy and Standard Management Process
- Information Security Policy Definitions Document
- IS-00.00 Information Security Policy
- IS-00.01 Information Security Risk Management Policy
- IS-01.01 Asset Management Policy
- IS-02.01 Information Classification Policy
- IS-03.01 Access Control Policy
- IS-04 02 Acceptable Use Policy
- IS-04 07 End User Computing Policy
- IS-05 00 IHS Markit Security Exception Process Policy
- IS-05 06 Patch Management Policy
- IS-05.03 Malware Protection Policy
- IS-05.07 Vulnerability Management Policy
- IS-05.08 Logging and Monitoring Policy
- IS-05.10 Network Security Policy
- IS-05.17 Mobile Device Management Policy
- IS-06.01 Cryptography Key Management Policy
- IS-07.01 System Acquisition, Development Maintenance Policy
- IS-08.05 Cloud Security Policy
- IS-09.03 High Risk Travel Policy
- IS-10.01 Business Continuity and Disaster Recovery Policy
- IS-11.01 Information Security Incident Management Policy

- Patching and Vulnerability Management Standard
- Secure Application Development Standard
- Email FAQ Guidelines
- Open Source Software Procedure

Ownership

Document Management:

Policy Name	IHS Markit Information Security Overview - External Facing
Policy Owner/Approval	Chief Information Security Officer and IHS Markit Information Security
Applies To	IHS Markit employees and third-party representatives worldwide
Date policy was last reviewed	June 2018