Information Security Overview

For external stakeholders

Last revision: February 2021

Original publish date: June 2018

Information Security Strategy and Vision

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

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

- Protect data and information assets against unauthorised access
- Assure the confidentiality of IHS Markit and client confidential information
- Maintain the integrity of IHS Markit data and information assets including annually conducting scheduled penetration and vulnerability audits on our systems
- Manage IHS Markit information systems in accordance with best practice and comply with legal and regulatory requirements
- Commit to incorporating relevant industry standards and data safeguards including, but not limited to, use of encryption technologies such as SSL/TLS (Secure Socket Layer, Transport Layer Security), differential privacy, and multi-factor authentication
- Produce, maintain and test business continuity plans to protect the continuity of control and availability of IHS Markit information assets and systems
- Ensure our employees receive information security awareness training and the resources to address potential data security threats
- Report, investigate and escalate, where appropriate, all information security breaches, whether actual or suspected, internal or external
- Ensure that critical vendors implement information security controls that meet IHS Markit information security requirements

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.

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 address the security risks and identify security requirements for systems and data.

The IHS Markit Information Security Control Framework reflects eleven core control domains. 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 enables IHS Markit to demonstrate the safe and effective management of data and services. Our core control domains are:

- Governance and Management

- Risk and Compliance
- Asset Management
- Protective Technologies
- Identity Management and Access Control
- Data Management
- Change Management
- Security Incident Management
- Vendor Management
- Physical Security
- Business Continuity Management & Disaster Recovery

The selection, development and management of our core control domains are based on industry frameworks. The Information Security Framework was designed to address the risks and security needs of the organization. We align with the following international standards in the development of this framework:

- ISO27001:2013 - Information Security Management System requirements
- ISO27005:2011 - Information Security Risk Management
- ISO27014:2013 - Governance of Information Security
- COSO Internal Control Integrated Framework
- NIST - National Institute of Standards and Technology Information Security Handbook - Cyber Security Framework
- PCI-DSS - Payment Card Industry Data Security Standard

Certifications/External Audits:

- ISO 27001 certification for our Polk automotive business line in North America. Certification is granted by a certifying body and requires both an internal audit and an external audit. This certification covers a 3-year period with audits occurring every year
- Numerous SOC 1 and SOC 2 (System and Organization Controls) external audits annually within our business lines. These assessments ensure appropriate controls are in place and that our customer data is secure and protected. Depending on the business line, we can also be assessed on our controls around customer confidentiality and privacy
- Annual financial audit towards compliance with the Sarbanes-Oxley Act of 2002 (SOX). This includes assessing our existing IT infrastructure and the management of potential security risks

Governance

Our Chief Information Security Officer (CISO) is responsible for policy development and strategy, compliance, assurance, monitoring and incident response.

The CISO reports to our senior leadership team and our Board of Directors including:

- Executive Vice President and General Counsel
- Risk Committee of the IHS Markit Board of Directors

Our CISO 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.

The Risk Committee reports to the Board of Directors periodically regarding IHS Markit's risk assessment and management program, including our cybersecurity program and data protection controls.

Security Incident Response

Our cyber incident response team (CIRT) is responsible for leading, coordinating and supporting responses to cybersecurity threats and data breaches, including incidents involving personal or sensitive information. The team is lead by the CIRT manager with guidance and support from the crisis management team (CMT). The CMT is the decision-making body that has been delegated authority by the executive committee to lead and respond to a crisis.

- **Incident response:** Our incident response methodology follows the guidance outlined in the NIST 800.61. Steps include (1) Preparation: developing the framework and resources the incident response team needs, prior to the detection of an actual Incident; (2) Detection and analysis: detecting incidents as they occur and examining the facts presented to determine the scope and impact of the incident; (3) Containment, eradication & recovery: taking steps to contain the impact of the Incident including eradicating the threat posed and recovering the affected systems, networks, and other company assets; (4) Post-incident activity: preserving evidence as needed and implementing steps to improve the company's cybersecurity posture
- **Notifications to stakeholders:** The CMT decides (1) whether notifications are necessary based upon legal requirements and industry practices; (2) the content of such notifications; and (3) which external parties need to be notified in a timely manner. These parties may include law enforcement, regulatory agencies, our data security insurance provider, consumer reporting or credit agency, and customers.

Employee Awareness, Training & Protections

IHS Markit employees are our first line of defense, and by taking a proactive stance and learning how to prevent threats, we can keep our organization safer. We have also taken steps to protect our employees against data security threats including:

- **Annual employee training:** All current and new IHS Markit employees conduct and attest to completing our annual cybersecurity awareness, annual SOX compliance, 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.

- **Phishing simulations:** Annually, we conduct quarterly phishing simulations that imitate real attacks so colleagues can better spot spear-phishing attacks, both at home and the workplace.
- **Report Message button:** Employees can readily report suspicious emails in Outlook to Microsoft allowing Microsoft to hone email filters to remove spam and phishing emails
- **Employee educational resources:** Employees have access to a library of IT security knowledge and techniques including a dedicated intranet site and a monthly cybersecurity awareness newsletter; a Phish Tank containing example phishing emails and a verified safe email repository; resources around vishing; and additional training for employees who need more training after our phishing simulations
- **Protecting corporate computer and mobile equipment:** All computers have anti-virus and firewall protection and receive automated Windows patching as needed. Access to computers is protected by user authentication and all data is encrypted. Mobile phones use a mobile device management application that protects IHS Markit content. In 2020 we completed the rollout of URL and web content filtering software on all corporate computers, enabling us to manage a safer online presence and reduce our risk from malicious websites and phishing attacks aimed at stealing both personal and corporate information
- **USB blocking:** To protect against malicious software and reduce the proliferation of IHS Markit data, all data transfer access to USB ports on corporate laptops and desktops is blocked

Privacy

We are committed to safeguarding the data and privacy of clients, employees and third parties according to IHS Markit's published privacy policies posted here: (https://ihsmarkit.com/Legal/privacy.html).

Records Retention

All IHS Markit employees, and applicable third parties who have access to IHS Markit and client information assets, are required to handle company records in accordance with applicable law and best practices. Records are stored, retained and destroyed according to their level of confidentiality. Records of higher confidentiality are protected by measures such as physical access restrictions, user authentication and encryption. Some highlights of our program include:

- **Email and messaging systems:** records are automatically deleted after 18 months
- **Records with 'Internal' classification:** records such as procedures and training manuals are stored in file directories and databases that require user authentication. Physical records are shredded. The disposal of electronic records is coordinated with the IT department to ensure permanent disposal
- **Records with 'Confidential' classification:** records such as PII, financial statements and IT system configuration records are stored using approved encryption methods, physical access restrictions and limited access to specifically authenticated and authorized employees. For destruction and disposal, confidential records are transformed into an unreadable state that cannot be reconstituted: paper copies are placed in confidential waste bins that are cross-cut shredded, pulped or burnt; records stored on hard drives are demagnetized before disposal or the media itself is destroyed; electronic records are rendered non-recoverable even against forensic data recovery techniques and their disposal is coordinated with the IT department

- **Retention schedules:** records within our retention schedule fall into two main categories:1) Destroyed after a specified period such as “destroy after 3 years”; 2) Permanently preserved such as IHS Markit bylaws or incorporation records
- **Legal holds:** IHS Markit will preserve all potentially relevant records if it becomes aware of pending or reasonably anticipated litigation, government investigation or audit

Information Security Policies, Standards, Guidelines and Procedures

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

- Access Control Policy
- Asset Management Policy
- Audio/Video Conferencing Standard
- Business Continuity and Disaster Recovery Policy
- Cloud Security Policy
- Cryptography and Key Management Policy
- Electronic Communication and Acceptable Use of Systems Policy
- End User Computing Policy
- Global Mobile Phone Policy
- Cybersecurity Incident Response Plan
- Data Leak Prevention
- Digital Forensics Policy
- Information Classification Policy
- Information Security Statement of Applicability
- Information Security Incident Management Policy
- Information Security Policy
- Information Security Risk Management Policy
- Logging and Monitoring Policy
- Malware Protection Policy
- Mobile Device Security Management Policy
- Network Security Policy

- Password Standard Policy
- Patch Management Policy
- Records Retention and Disposal Policy
- Records Retention and Disposal Policy: Records Retention Schedule
- Records Retention and Disposal Policy: Index of Record Types
- Security Awareness Training Policy
- System Acquisition, Development Maintenance Policy
- Travel Risk Management Tools
- Vulnerability Management Policy

Document Management

Name	IHS Markit Information Security Overview
Owner/Approval	VP, Information Security
Applies To	IHS Markit employees and applicable third-party representatives worldwide who have access to IHS Markit's systems, information, intellectual property, and data
Date last reviewed	February 2021