Security Practice Overview

January 2023

Table of Contents

Information Security Practices

Morningstar is committed to taking reasonable efforts to secure the confidential information, assets, and intellectual property that belong to Morningstar and its clients. A number of different threats exist that endanger the confidentiality, integrity, and availability of Morningstar information. In order effectively protect our information assets, employees, contractors, vendors, and third parties with access to the Morningstar network or Morningstar owned/managed facilities are required to abide by Morningstar Information Security Policies.

Information Security Team

Morningstar has a global information security team dedicated to protecting Morningstar's information assets. Morningstar's Chief Information Security Officer leads the information security team and is responsible for IT risk governance, software and product security, security operations and incident management, IT compliance, technical disaster recovery, and determining enterprise-wide security policies and procedures. The information security team is staffed with experienced professionals in each of these areas. Morningstar's CISO reports to the Chief Technology Officer and also reports progress quarterly to Morningstar's Board of Directors.

Hiring Practices

Morningstar adheres to all local, state, and federal laws regarding hiring and employment practices. We strive to maintain a standard of excellence in its practices that minimizes risk associated with the employment relationship. Candidates often go through several rounds of interviews. The experience and skill of candidates for employment are evaluated before they assume the responsibilities of their position. All employees are subject to a mandatory pre-employment background screening. Non-employees (e.g., consultants, vendors, etc.) who are granted certain access to Morningstar buildings, personnel, or technology are required to go through a similar background screening process prior to providing services. Employees and non-employees in non-U.S. offices are subject to background screening as provided for by local law.

Information Security Policies

Morningstar's Information Security Policy and Standards define information classification, appropriate data handling and usage, roles and responsibilities, access controls and provisioning, logging, monitoring, cryptography and key management, security awareness, virus prevention, risk assessments, physical security, mobile device policy, network security, vulnerability management, policy enforcement, and handling of exceptions. Policies are aligned with ISO 27001:2013 and NIST SP-800 publications. Each year the Chief Information Security Officer reviews and approves the Information Security Policy.

Information Classification

Morningstar's Information Classification policy establishes requirements for classifying and handling information across Morningstar regardless of the form it takes (physical, digital, etc.). Information is grouped into one of the following four categories: Restricted, Confidential, Internal, or Public. Handling requirements include, but are not limited to, acceptable encryption, distribution, transmission, storage and disposal methods depending on the classification level. The Information Classification policy prohibits transferring sensitive, non-public information unencrypted over public networks (e.g. Internet). Personal Information is classified as Confidential or Restricted Information (depending on the data elements). Morningstar policies and processes ensure that data classification and handling to meet the requirements of the European Union General Data Protection Regulation (GDPR) and other applicable privacy regulations.

Acceptable Use

The Internet and Network Acceptable Use Policy outlines the acceptable use of Morningstar's network and computing resources. The scope of the policy includes, but is not limited to, use of the Morningstar network, Internet, email systems, wikis, Intranet, instant messaging applications, and all other information systems and company electronic communications mediums. The policy applies to all employees, contractors, consultants, and other individuals at Morningstar, including all personnel affiliated with third parties. It covers all equipment that is owned or leased by Morningstar or connected to Morningstar's network.

Asset Classification and Management

Morningstar has procedures in place to approve and maintain hardware and software inventories to minimize loss due to theft, destruction or other damage. Distributed assets are identified with owners and maintained in Morningstar's IT Catalog, a system inventory application. Asset type, format, location, ownership, installed software versions and information classification is documented where applicable. Technology Managers and/or asset owners are responsible for updating and maintaining the accuracy of inventories (such as ownership, asset retirement/decommissioning, software versions) and reporting loss, theft or damage of assets.

Policy Communication

Morningstar communicates security and confidentiality obligations including security policies and ethics guidelines to employees on an annual basis. Upon hire, and then annually thereafter, employees must formally acknowledge that they have reviewed and will comply with Morningstar's Information Security Policy. Policies and procedures related to security and confidentiality are made available to employees through email, training, and internal websites. Management promotes these policies in management meetings, communications, and leading by example.

Failure to comply with policies and procedures can result in disciplinary action, up to and including termination of employment, removal of contract personnel and/or initiation of appropriate legal action.

Security Awareness Training

Upon hire and at least once annually, we require Morningstar employees to complete security awareness training. Awareness topics addressed in training include company security policies, acceptable use, physical security, data privacy, information handling, social engineering, phishing, email, password use, virus and malware protection, and other good security practices. Notifications are sent to non-compliant employees until course completion.

Phishing Exercises

Morningstar conducts quarterly phishing exercises to test our employees' ability to detect phishing messages. Employees who are compromised as part of these exercises are automatically enrolled into additional social engineering and phishing awareness training. Morningstar tracks the results of the phishing exercises and report them to senior management quarterly.

Logical and Physical Security

Morningstar has established policies and procedures for logical and physical security, which includes restricting access to programs, data, networks, and other information resources. Morningstar uses a combination of manual and automated controls to enforce our policies. We design our policies, standards, and operational procedures to mitigate the potential risks to Morningstar and client data.

Access Management

Morningstar's access control policy establishes a means to control logical access to information systems, and resources. The major components covered in this policy include user account management, privilege user access, password management, review of access rights, and the use of generic accounts. Access control rules incorporate the principle of least privilege, which grants the appropriate level of access required for an individual's specific role.

Employees, contractors, and vendors who require access to Morningstar information systems and network are assigned unique IDs to ensure accountability and traceability; the use of shared accounts is strictly prohibited. Users who require access to systems and applications must open an access request and obtain approval from system owners before access is granted. Segregation of duties is enforced so that the person requesting or approving access is separate from the person provisioning access.

Privileged Accounts

Rights to perform system administration to programs, data, and other information resources are restricted to employees with a valid business need. Privilege users are given a separate account to perform system administration and are not permitted to use their regular user account. All administrative account credentials are stored in a secure credential management tool. The credentials must be checked-out daily and are configured to utilize multi-factor authentication upon account check-out. The accounts' passwords are valid for twelve (12) hours and automatically rotate upon account check-in. System owners review privileged administrative access on a quarterly basis.

Remote Access

Employees are provided access to the Morningstar network via a Virtual Private Network (VPN) which enforces two-factor authentication. Employees can only connect to the network with a Morningstar issued device. Morningstar provides access to an encrypted web-based corporate email system which enforces two-factor authentication.

Termination Procedures

Morningstar uses Workday to initiate personnel termination processes. Human Resources personnel enter the termination request into Workday. All termination transactions automatically initiate the disablement of Active Directory accounts, which disable all access to Okta (SSO for internal resources), application servers, email, and virtual private network (VPN). Active Directory accounts are disabled within 24 hours of notification of termination. Service desk tickets are generated to the appropriate team to remove physical access and reclaim assets. Logs of all activities are available in Workday, our corporate service desk system, and our identity and access management solution.

Password Management

Morningstar has implemented password management controls in compliance with corporate standards that include minimum length, expiration, complexity, and account lockout. In addition, default vendor or system passwords must be changed following installation of software. Temporary passwords (resulting from a password reset or initial account creation) must be unique and changed after first login.

Password Policy for Internal Systems (Windows Domain)

- Minimum 8 non-sequential characters
- Expires after 60 days
- Must contain three out of the following—at least one upper case, one lower case, one numeric digit, or one special character (e.g. ! * # $)
- Lock after 5 failed login attempts
- Lock after 15 minutes of inactivity
- Last 8 passwords cannot be used
- Passwords cannot contain any part of username

Encryption

Morningstar uses strong encryption to protect transmission of user authentication and other confidential information passed over public networks (e.g. Internet). We enable industry standard TLS protocols to ensure the privacy of data as it moves between the user's browser and our web servers. Highly sensitive information (credit card numbers, passwords, Social Security numbers, etc.) stored in electronic format requires encryption in transmission and storage, and must be stored on Morningstar equipment.

Intrusion Detection

Morningstar maintains a robust perimeter security program using an intrusion detection system (IDS). This system monitors Morningstar's external perimeter and reports security events to dedicated consoles. The data generated by this system is reviewed daily by our Security Operations

Center. Alerts that require further investigation are escalated to Information Security Department members, who provide response capability and analysis on Internet-based threats.

Firewalls

Morningstar has firewalls in place to prevent unauthorized access to the network. Morningstar's Information Security team reviews and approves firewall rules and ports prior to implementation. Ports and services are limited to those that are necessary to provide services. In Amazon, Morningstar utilizes network access control lists and security groups to prevent unauthorized access to the cloud environment. Morningstar's Information Security team reviews and approves rules and ports. Ports and services are limited to those that are necessary to provide services.

Network Monitoring

Morningstar's security event monitoring process runs 24x7x365 and produces alerts and reports for review and mitigation, if necessary. The Information Security Department reviews various security event logs, including alert data generated by the network intrusion detection sensors and the centralized logging server, on a daily basis. Alerts are configured to identify common potential network-based security attacks to the system.

Virus Prevention

All Windows and Mac-based workstations and servers connected to the Morningstar network are required to have antivirus and endpoint detection/response software installed, configured, activated, and updated with the latest version of virus definitions before or immediately upon connecting to the network. Virus signature definition updates are distributed to servers and workstations as they become available. Alerts triggered by the antivirus clients are sent to a centralized console and the Information Security Department reviews them as needed. If necessary to prevent viral propagation, infected computers are disconnected from the network until the infection has been removed.

Web Content Filtering

Morningstar currently uses a web proxy and content filtering platform to control outbound Internet traffic from user workstations and to enforce corporate security policies across our network. The web filter categorizes billions of web pages in more than 50 languages into 85 useful categories that can be blocked or allowed depending on the policies we apply. Morningstar blocks sites categorized as hacking, malicious content, malware, peer-to-peer (P2P), phishing, piracy, proxy avoidance, violence/hate/racism, spam, adult content, nudity, scams, controlled substances, and illegal activity. The platform offers DNS-layer security separately to simplify security for businesses of all sizes.

Patch Management

Morningstar has established a patch management policy addressing the deployment of security and confidentiality patches to systems. We deploy operating system security and confidentiality patches to desktop and server workstations on a monthly basis. We release patches into test environments to ensure compatibility and stability is maintained before we distribute them to live production environments. In Amazon patches are deployed on a monthly cadence either via our Patch

Management system or via an application redeployment using a freshly patched server image. Patches and redeployments are rolled up and tested through each environment to minimize any impact to the production environment.

Vulnerability Management

Morningstar's Information Security Department conducts routine vulnerability scans of operating systems, network devices, and web-facing applications. Once a vulnerability assessment is complete, we present results to information and technical owners for remediation and/or risk acceptance. Information Security tracks vulnerabilities from identification to closure.

Application Security Testing

During development and prior to each release of an application, the Information Security team performs an automated Static Analysis scan, Dynamic Analysis and Penetration Testing on source code to identify common security vulnerabilities. Additionally, application source code is scanned on a weekly basis and vulnerabilities are reported to product teams on their product scorecards.

Assessment findings are ranked by severity and entered into our bug-tracking system. The Information Security team reviews vulnerabilities with application development teams and provides a clear set of remediation instructions. A summary of the vulnerabilities and their associated risk ratings are presented to management for review on a weekly basis as part of a Product Scorecard. The application vulnerabilities and associated remediation timeline are also reviewed with the business and product line leadership as part of regular Product Scorecard reviews.

Secure Software Development Lifecycle Morningstar has established a Secure Software Development Lifecycle (SSDLC), which requires all changes that may affect the security or confidentiality of the system to be reviewed by the Information Security Department before release.

The Security Questionnaire, a CAB deliverable, is completed by each technical product owner during the design phase of every project and requires the documentation of changes to key security elements such as authentication and authorization controls, key management functions, logging and monitoring controls, cryptographic functions, logical security controls, infrastructure or firewall rules, information classification and handling controls and compliance/regulatory controls. Once documented, a member of the Information Security department reviews the Security Questionnaire for any material security or confidentiality risk to the system. The Information Security department completes a security and confidentiality risk assessment and identifies, and rates potential risks based on severity. Management must accept or remediate risks before completion of the project.

Application source code and corresponding configuration data is stored within a centralized code versioning repository. All changes to the versioning repository are logged. Before deploying a release into the live production environment, Quality Assurance personnel test the source code for defects. Once Quality Assurance personnel sign off with approval to release, a release ticket is created requesting the deployment of code into the live production environment. Development and testing is performed in an environment that is separate from the production environment.

System Security Hardening

Server creation and security hardening procedures outline steps for sever creation, standard settings, configurations, and account policies. Security hardening settings are applied and enforced using configuration management software. The Information Security team reviews security hardening procedures annually.

Physical Security

Access to Morningstar offices is granted on a least privilege basis. Employee security badges and card readers control access to each office. Visitors must first register with building security and must provide valid government-issued identification prior to being allowed access. Visitors are presented with a visitor sticker and must always be escorted by a Morningstar employee. Temporary security badges with limited hours of access are available for pre-authorized visitors and vendors who require extended access.

Access to Morningstar on-premise data centers and processing facilities is strictly controlled. Key card readers linked to employee security badges control physical access. Data centers are equipped with on-site security guards and video surveillance at all entrances and exits. Access is granted to employees who require access on a regular basis to perform their job functions, and is reviewed on a quarterly basis. Should a non-authorized individual or visitor require temporary access to a restricted area such as a data center, they must first sign in and an authorized Morningstar employee must accompany the visitor at all times. All access attempts are logged and retained for at least 90 days.

Environmental Controls

Morningstar on-premise data centers are equipped with the following environmental controls: temperature and humidity detection equipment, leak detection equipment, heating, ventilation and air conditioning ("HVAC"), uninterruptible power supply ("UPS"), redundant power feeds, fire detection systems, handheld fire extinguishers, raised floors to facilitate cooling, and pre-action dry pipe water sprinklers. Morningstar has defined thresholds for monitoring temperature levels, humidity levels, and power/water leak detection. If one of the thresholds is exceeded, it triggers an alert, and facilities and technology personnel respond to assess and resolve the issue. On an annual basis, management contracts third-party vendors to complete fire, humidity, temperature, and leak detection, and fire suppression equipment inspections.

Service Operations Center

The 24x7 Service Operations Center is equipped with the tools and resources necessary to closely monitor environmental protections and core infrastructure health, and maintain system uptime. This team's responsibilities include incident management and event management.

Product Scorecards

Each Morningstar product receives a scorecard on a weekly basis that measures and tracks security posture, product disaster recovery, incidents, changes, and basic operational readiness. The

scorecard is intended to rate the product's risk level and overall health by considering all types of issues existing within the application, as well as the type of information the application processes.

Product scorecards assign a rating in multiple areas, including security, disaster recovery, technology operations, infrastructure operations, and service operations. The security rating includes vulnerability data from penetration tests, static analysis scans, and vulnerability scans which is aggregated and surfaced as part of the Scorecard. The security rating for each product is based on the vulnerabilities open, the type of information processed, and whether vulnerabilities are remediated within the timelines specified in our security policy.

Ratings are surfaced to technical product owners and business leads on a weekly basis and product team goals and objectives include minimum rating criteria for the year.

Vendor Risk Management

Morningstar performs comprehensive Information Security due diligence assessments on critical vendors, subcontractors, and other third parties that may process confidential information prior to conducting business with them. Business units submit requests for engagement with vendors to the Information Security team along with information about the engagement such as the data being processed by the vendor and the storage location of the data. The information submitted by the business unit is used by the Information Security team to tier the vendor and determine the depth and frequency of the Information Security due diligence assessment. As part of this assessment, the Information Security team will provide the potential vendor with a security questionnaire and ask for security artifacts such as an SSAE 18 SOC2 report and external penetration test. Upon return, the team will review the questionnaire and all available security documents. Policy gaps or risks are highlighted and routed to the business owner. The business unit then reviews the risk assessment and defines a risk mitigation or risk acceptance plan for review with Information Security, if needed. Contracts with third parties include a required set of security controls that third parties must agree to maintain throughout the course of the engagement with Morningstar.

Incident Management

Morningstar's Security Incident Management Policy serves to minimize the impact and consequences of security and infrastructure related incidents; improve our ability to restore operations resulting from an incident; and ensure appropriate parties are promptly notified so that incidents are handled in a consistent and timely manner.

The Security Incident Management Policy covers information security incidents such as unauthorized access to a system or database, violations by an internal employee of the acceptable use or information security policies, the introduction of viruses or malicious code, denial of service attacks, and/or loss or theft of information. Incidents are ranked according to whether sensitive information is involved, how widespread the incident is, how much the incident impacts customers or business partners, whether the incident affects critical enterprise infrastructure resources or has

the potential to raise public attention, involves active threats that could cause severe impact, and/or involves breach of contract or other legal impacts.

The policy creates an Incident Management and Response team to respond to and mitigate all incidents. This team may consist of representatives from management, infrastructure, information security, corporate communications, business unit leadership, client relationship management, and human resources, depending on the scope and severity of the incident. The policy requires that all suspected policy violations, system intrusions, virus infestations, or other conditions that might jeopardize information or systems must be immediately reported to the Information Security Department. All incidents that affect the availability or integrity of our networks or computing resources must be reported to our Service Operations Center.

During an incident, the Incident Management and Response Team will start the analysis and recovery phase to direct triage, response, and recovery; provide technical support and expertise related to impact assessment, incident handling, and technical system management; report incidents to appropriate internal management teams and/or authorities as required; record incident details using Morningstar's standard incident report templates; and prepare external/internal communications and updates. The team will then use Morningstar's standard root cause analysis template to determine what controls or procedures can be put into place to prevent the incidents from reoccurring.

The Incident Management and Response Team conducts annual incident response exercises to test the effectiveness of our response capabilities.

Change Management

Morningstar's applications and IT infrastructure components are subject to formal change management processes and procedures. Change management procedures ensure that changes to systems and applications are performed in a predictable and orderly manner. Changes are logged, scheduled, tested, approved, and communicated to system owners prior to implementation.

Development and QA testing is performed in an environment that is separate from the production environment. The Change Activity Board (CAB) and application owners review and approve change requests before release. Additionally, the Information Security team reviews changes that have the potential to affect the security and/or confidentiality of Morningstar systems.

Security and Privacy Advisory Council

Morningstar's Security and Privacy Advisory Council meets on a quarterly basis to discuss environmental, regulatory, and technological changes and associated risk to security and confidentiality of the organization's information. This meeting is co-chaired by the Chief Information Security Officer and Directory of Privacy and consists of executive management from the Information Technology, Legal, Audit, and Compliance departments. Council meetings provide a forum for the cross-functional, global identification and resolution of security issues, endorsement of security strategies, and review of significant exceptions to information privacy and security policy. The Security and Privacy Advisory Council also works to identify key corporate security

initiatives and standards (for example, virus protection, data classification, security monitoring, intrusion detection, access control to applications and facilities, and remote access policies).

Cyber Security Intelligence

The Information Security team includes seasoned security professionals who provide response capability, analysis, and broad intelligence on cybersecurity threats. They subscribe to many information security websites and attend industry conferences to keep current with the latest cyber security vulnerabilities and trends. The Morningstar Information Security team is also a member of the Financial Services Information Sharing and Analysis Center (FS-ISAC) and receives daily critical security alerts, threat notifications, and XML data feeds used in threat analysis.

Cyber intelligence is a continual, iterative process of obtaining, analyzing, and sharing threat information. The Information Security team places a great deal of importance on effectively communicating threats and vulnerabilities internally with its employees and externally with customers and shareholders.

Cybersecurity Insurance

Morningstar carries insurance coverage policy for cybersecurity-related incidents. Morningstar periodically reviews this coverage in association with Morningstar's risk assessment processes to ensure it is sufficient to cover the firm in the event of an incident.