MathWorks
Accelerating the pace of engineering and science

MathWorks Information Security Practices

The information security program at MathWorks draws from several industry-standard frameworks, including ISO 27001 and the NIST Cybersecurity Framework. It is the policy of MathWorks to protect customer, employee, partner, and corporate information from unauthorized access. MathWorks has full-time information and product security departments that regularly report to executive management. MathWorks uses risk management techniques to align security activities with relevant risks to our business and data. Security responsibilities get broad communication within the organization. MathWorks maintains an internal quality assurance function to assess the performance of internal controls and regularly reports results to executive management. MathWorks continually improves our information security program as part of ***our core values***.

Security Policies

MathWorks maintains policies to support our information security program. These policies address acceptable use of technology, data storage, access control, incident response, employee training, as well as privacy and protection of personally identifiable information. Executive management reviews and approves policies on a regular basis.

Organization of Information Security

MathWorks has full-time departments for information and product security. Responsibilities are assigned by executive management. Security teams report on objectives and performance of the program. To reduce opportunities for unauthorized access to assets, teams take care to segregate their duties.

Human Resources Security

MathWorks conducts background verification checks on candidates for employment. All MathWorks employees are required to acknowledge a confidentiality agreement upon hire. Management communicates security responsibilities to employees and contractors. MathWorks maintains an information security awareness and training program. Training is given as part of new hire orientation and on a regular basis thereafter. Specialized information security training is provided based on job functions.

Asset Management

MathWorks maintains asset inventories to support information security objectives. Acceptable use of assets is defined in policies that are communicated to employees. MathWorks reclaims corporate assets upon termination of employment.

MathWorks defines criteria for classifying information assets based on criticality and sensitivity to unauthorized access. Standards support asset classification by enumerating information security requirements. MathWorks uses asset disposal vendors to securely dispose of assets upon retirement.

Access Control

MathWorks implements access control policies and procedures to follow the principles of least privilege and need-to-know. Access to MathWorks managed information requires a username and password. Remote access to the MathWorks private network requires multifactor authentication. Password composition requirements observe industry best practices. Procedures document the process for provisioning and deprovisioning user access. Allocation and use of privileged access rights use restrictions. MathWorks has policies, procedures, and technology to support the management of secrets, including passwords, API keys, and digital certificates.

Cryptography

MathWorks maintains cryptographic standards to protect information, encrypting information both at-rest and in-transit. MathWorks maintains a secure file transfer portal for communicating with external parties based on use case.

Physical and Environmental Security

Access to MathWorks offices and information processing facilities is restricted. Sensitive areas like data centers and telecommunications rooms are further restricted to authorized personnel based on job requirements. MathWorks headquarters has 24x7 guard presence and security alarm monitoring. MathWorks managed data centers have standard environmental protections against fire, water, power loss, and other environmental hazards.

Operations Security

MathWorks maintains documented operating procedures to support information security objectives. Procedures define processes for configuring operating systems and network equipment, maintenance, change management, malware protection and removal, and incident response. Development and test environments are segregated from production. MathWorks has a comprehensive log monitoring process that collects logs centrally checks them for anomalous behavior. MathWorks maintains a vulnerability assessment and remediation program.

Communications Security

MathWorks implements security controls on network perimeters, including on-premises and cloud infrastructure. Network segmentation controls limit access to required endpoints and protocols. MathWorks wireless networks use enterprise security controls to encrypt communications and limit access to authorized users only.

Systems Acquisition, Development, and Maintenance

MathWorks follows security procedures to acquire, develop, and maintain information systems. Our secure software development standards draw from several best practices, including OWASP, Microsoft Secure Development Lifecycle, the BSA Framework for Secure Software, and the NIST Secure Software Development Framework (SSDF). Our processes include developer training, application security best practices, secure coding standards, security testing, and application security vulnerability assessments.

Supplier Relationships

MathWorks suppliers are contractually obligated to comply with laws and implement required security and privacy safeguards. Before granting access to data or systems, MathWorks conducts a security evaluation of all suppliers.

Information Security Incident Management

MathWorks maintains a program for managing information security incidents. This program includes documented roles and responsibilities, response procedures, reporting requirements, and a root cause analysis process. MathWorks conducts tabletop exercises to practice its response to information security incidents on a regular basis.

Business Continuity Management

MathWorks is organized around critical business practices for development, support, sales, and other corporate activities. As a global organization, MathWorks executes these activities from multiple locations. In the event of a regional disaster or significant system outage, it is our practice to manage critical functions from an alternate location. System availability and recoverability are core design principles of our information systems architecture. Critical information systems are designed to minimize the risk of downtime and, if needed, recover required functionality to manage key business operations.

Compliance

MathWorks complies with legal, statutory, and regulatory obligations related to information security. MathWorks maintains an internal quality assurance function to assess the performance of internal controls and regularly reports results to executive management.