Arm Security Program

Arm Security Program

Arm has built an effective security program that centers around technical controls and empowering our people to be our best line of defense. Our security program focuses on four main areas: Identify, Protect, Detect and Respond, and Recovery.

Identify

Risk Management

Arm has a robust security risk-management program which includes regular risk assessments, evaluation, tracking of mitigation in risk registers, and escalation to the highest level of the organization to aid in prioritization decisions.

Governance

Security Governance extends from an enterprise-wide security council to line management and up to the executive committee to ensure visibility and support of security risks, issues, and decisions.

Policies & Procedures

Arm maintains a set of information security policies based upon the National Institute of Standards and Technology (NIST) Cyber Security Framework and ISO 27001:2013. Each line of business may have unique policies and standards that provide a higher level of security than the baseline established by the enterprise-wide policy framework.

Asset Management

Arm takes a systematic approach to managing our tangible and intangible assets throughout their lifecycle to ensure their security from inception to destruction.

People Security

Arm seeks to guide employee behavior through three core beliefs:

- We, not I
- Passion for progress
- Be your brilliant self

The Arm beliefs are reinforced by our Acceptable Use Policy and Code of Conduct. All employees are subject to background checks and NDAs.

Third Party Onboarding and Monitoring

Security and privacy apply a risk rating at onboarding based upon the supplier type and responses to a standard questionnaire. During implementation, the security team provides and monitors adherence to security best practices to ensure that Arm's exposure to third-party security breaches is minimized.

Protect

Training and Awareness

In addition to the annual security awareness training, Arm conducts training and awareness campaigns throughout the year that engage employees and raise awareness around relevant threats. The Security Champion program has built advocates for security across Arm to help deliver training and awareness quarterly.

Information & Data Management

Everyone at Arm must handle data held by Arm securely as highlighted in our Data Classification Policy, and everyone is responsible for ensuring they handle that data according to its security classification.

Physical Security

The Arm Security Council manages physical security through regular updates, roadmap reviews, and assigned engagement within the enterprise security team. Each office is appropriately equipped with badges, camera, security guards, and other relevant physical security controls.

Logical Security

Arm uses authentication technologies to control access to systems and components of its codebase. Arm administrators use two-factor authentication when logging in remotely and logging into Arm consoles controlling accounts with cloud service providers. Administrative access to the system requires a VPN connection and authentication to the servers with a secure shell ("SSH") public-private key pair. In addition, the system protects data at rest, either through encryption or strong access controls. The security team also documents anti-malware policies, procedures, technical standards, guidelines, and training materials.

Cloud Security

Arm has executed a strongly governed, cloud-first strategy to meet business objectives for speed, resiliency, and security. Under a shared responsibility model, Arm thoroughly reviews the cloud platform to establish a secure foundation, and the services and functions that Arm builds in the cloud follow the applicable Arm security policies and processes.

Secure Development Lifecycle

A secure development lifecycle is used to minimize security vulnerabilities in development. Arm considers security and privacy throughout the entire development lifecycle, enabling Arm to work on the elimination of vulnerabilities at an early stage. Arm's secure development lifecycle requires all products have a living threat model that identifies security objectives for new development.

Change Management Process

Changes to systems and their supporting services are planned by the product engineering teams as part of a regular planning process or in response to customer, regulatory, and/or business priorities. Arm uses an agile development methodology to manage tasks within team-based development environments.

Vulnerability Program

Security is a top priority at Arm, and we welcome feedback from researchers and the security community to improve the security of products and services. We operate a coordinated disclosure policy for managing vulnerabilities and other security issues, and for quickly providing advice and mitigation. Read more about the security reporting process, and get the latest news, information, and updates about security exploits, such as denial-of-service, side-channel and Rowhammer attacks.

In addition, Arm has a robust vulnerability management program whereby servers are patched per an agreed SLA based upon criticality to ensure that the latest security vulnerabilities do not put Arm at risk.

Data Security

There are established data security practices for hardware and software in place that protect data from unauthorized access and corruption throughout its lifecycle. This includes, but is not limited to, encryption, key management, and training our people.

Backups

Backups are completed in accordance with our policies. Data is backed up per policy and encrypted across multiple locations.

Detect and Respond

Detection

Arm has a global 24/7 cyber detection and response capability that uses a suite of innovative methods and tooling to detect cyber threats across the estate. Log reviews and ongoing monitoring to identify anomalies are conducted daily. Upon detection, threats are contained swiftly against aggressive SLAs and the intelligence is shared to the wider community.

Respond

In the event of a cybersecurity incident, Arm is committed to ensuring that response processes are followed. Communications to the parties involved is sent in accordance with our SLA. The response team collaborates with the rest of the organization and has established crisis plans to ensure the entire organization can quickly come together to coordinate the necessary response and mitigate the risk as soon as possible.

Recovery

Business Continuity Plan

A business impact assessment is conducted to determine recovery time objectives, criticality, and requirements for plans to recover from a loss or disruption of the asset or service. Assets and services are protected with a BCP and disaster recovery plan which are tested annually.

Communications

Arm has a communications plan as part of the incident response and BCP plans. The communications plan helps ensure customers are informed of relevant incidents pursuant to their contractual, legal, and regulatory obligations. It is also part of Arm's on-going support for customer relationships.