QAD Security Overview

Our manufacturing and supply chain solutions help customers thrive in a competitive, high-risk and ever-changing world. We invest heavily in security and are committed to continual improvement. This overview describes how we deploy people, process and technology to ensure business continuity and the confidentiality, integrity and availability of data.

Governance

At QAD we follow a risk-based approach to integrating security across products and operations. Our Security Steering Committee sets the enterprise security strategy and oversees the execution of the security program. Information security policies and standards set the governance criteria for information security across QAD systems, employees, contractors, partners, customer environments and data. Our risk management process ensures tracking of the remediation and/or mitigation for all major security risk areas identified. QAD works closely with industry organizations, security analysts, CISA and law enforcement to stay current on the ever-evolving threat landscape and the proven methods of addressing such risks.

Security Engineering and Operational Controls

The Enterprise security program integrates industry best practices with the foundational set of security controls towards the objective of protecting availability, confidentiality and integrity of QAD customer data and systems.

- **Identity and Access Management** Identity lifecycle management and access control standards follow the principle of least-privilege and segregation of duties when granting end-users access to our systems. Access recertification is conducted for the existing entitlement grants on a periodic basis. Privileged access is managed through an elevated set of security controls and processes. All access to production systems is logged, tracked and monitored using best in class security technologies to identify and detect anomaly, correlate security exception events and alert our security operations team that triages such alerts using standard security procedures.
- **Zero Trust Framework** The principle of network segmentation and user segregation are followed at application and service layers to deliver defense-in-depth. All remote connectivity is through secure protocols. We deploy industry-leading tools and mechanisms to mitigate distributed denial of service attacks and maintain high availability. Data in transit is encrypted within all system configurations and across all communications. Backups are encrypted as well. QAD provides additional solutions to cover specific scenarios for data at rest encryption in the customer environments.
- **Threat and vulnerability management** QAD has defined security assessment programs including security testing and perimeter defense that leverage internal penetration testing teams and external industry experts to help us identify potential vulnerabilities within our environments and

products. We conduct periodic scanning of our hosts for vulnerabilities using industry-standard scanners and perform any required corrective action plans and mitigation efforts.

- **Disaster recovery and business continuity** Our plans are documented, communicated and reviewed annually for relevance and tested on a frequent basis. There is a well-defined change management process that applies to all deployment processes to ensure integrity and availability.
- **Incident management and response** We maintain procedures and 24x7x365 capacity for responding to security incidents. We regularly test and improve these capabilities across our entire enterprise, including internal and external stakeholders.
- **Secure disposal and destruction** We follow industry best practices in the secure disposal and destruction of equipment and media at end-of-life.

Security Operations

The 24x7x365 security operations team is responsible for monitoring emerging security threats daily, analyzing impact and appropriately responding to such threats by implementing security fixes and detections. This team is also responsible for sending any relevant communications to QAD users and customers on these security issues to ensure awareness and protective actions. As and when needed, the team follows standard escalation processes to coordinate with various stakeholders and external parties to protect our environments, services and customers.

Shared Security Model

Security and compliance within the QAD Cloud is a shared responsibility between QAD teams and our customers. In order to securely operate in the QAD Cloud, it is imperative that our customers know their security and compliance responsibilities. Principle among these responsibilities is staying on current versions per QAD's Product Lifecycle Policy and third-party lifecycle policies which makes it possible to apply necessary patches and other maintenance functions.

Physical Security

- QAD in partnership with its cloud providers is responsible for protecting the global infrastructure consisting of hardware, software, networking and facilities hosting its product and services platforms.

Infrastructure Security

- QAD is responsible for providing a secure network infrastructure including platform security, virtual private networking, load balancing, DNS and gateways.
- Customer is responsible for securely configuring and managing the virtual hosts, containers, storage, file systems, objects, etc. that are under Customer's control.
- Customer is also responsible for client and end-point security for the devices that access their resources on the QAD Cloud.
- QAD and our customers share the responsibility of ensuring optimal configurations of network access controls.

Workload Security

- QAD is responsible for providing secure systems that are hardened, protecting and securing the operating systems against attacks, patch management and vulnerability mitigations and remediations.
- Customer is responsible for protecting application layers via secure configurations and patching of applications and third-party tools.

Risk Management

- Customer is responsible for understanding the data classification, resource labeling and security requirements for the protection of customer assets. This includes evaluating the

relevant risk scenarios to identify risks and defining a security posture that is specific to managing these risks.

Identity and Access Management (IAM)

- QAD is responsible for providing identity lifecycle management, authentication, authorization and attestation services.
- Customer is responsible for human risk management for its personnel, including background checks and security awareness training for the individuals approved for access to customer cloud resources. Customer's responsibility also includes protection of cloud access credentials, privilege segregation and periodic reviews and attestations to ensure a controlled security posture within customer environments.

Secure Software Development Lifecycle

QAD understands that the integrity of its cloud services and products is of utmost importance to our customers and ensures that our products meet the industry standards for security so that customers deploy them with confidence. To achieve this QAD has established oversight procedures that identify and mitigate potential product security risks during the development lifecycle. To mitigate these risks to critical infrastructure, intellectual property and sensitive data as a result of the constantly evolving threat landscape, QAD has developed comprehensive and rigorous software security assurance processes and procedures. Our secure development best practices consistently apply secure methodologies and practices to every element of our product development lifecycle. We train the developers on secure design principles such as data validation, data privacy, vulnerability and threat management. We ensure that our product development standards evolve to keep ahead of the emerging issues and threats that affect code and the security of our products.

QAD objective is to delivery secure implementation and integration mechanism for our products via secure practices that include:

- Definition of product security requirements - authentication, authorization, encryption, network security, etc.
- Source code controls - access to the creation, modification, deletion and assembly of code into larger parts on a per-user basis
- Static code assessment plan and training
- Dynamic code analysis and build process integration
- Threat modeling - Identification of security flaws and design errors
- Open Source Software and Third-Party software validation - enabling fix for vulnerabilities prior to software releases
- Security testing and overall summary review

Personnel

QAD places a strong emphasis on personnel security with the objective of minimizing risks associated with human error, theft, fraud and misuse of facilities, including personnel screening, confidentiality agreements, security awareness education and training refreshed and renewed on an annual basis, and related policies that drive enforcement of disciplinary actions, if and when needed. QAD maintains high standards for ethical business conduct at every level of the organization, as applicable locally for each of its global locations. Our human risk management program includes comprehensive security awareness training programs that educate our users on core security topics for all new employees and annual refresher training for all. Additionally, there are various in-depth functional training sessions designed for specific job roles.

Partners and Suppliers

Partners and suppliers are contractually committed to equivalent security practices when granted access to QAD environments, systems and data. We conduct screening and oversight to identify and address risks.

Privacy

See our Privacy Overview to understand how we manage the processing of personal data.

Compliance

See the QAD Trust Center for a listing of certificates, reports and attestations that demonstrate our adherence to global industry compliance standards.

# # #