APPENDIX 3

ARDOQ INFORMATION SECURITY

1. Information Security Management System

1.1 Ardoq shall establish and develop an Information Security Management System (**ISMS**) encompassing policies, standards and procedures to ensure information security is addressed as part of the development and operation of the Ardoq Services. Ardoq reserves the right to update and develop the ISMS and the security measures listed herein without notifying the Customer in order to adapt to, among others, evolving industry standards, emerging technologies, cybersecurity threats, provided that such changes will not reduce the level of security described herein.

1.2 Ardoq shall perform an internal information security risk assessment at least annually and in any case in connection with significant organizational changes. Risk assessments shall follow a process modelled on NIST Special Publication 800-30 Revision 1.

2. Organizational Security

All Ardoq employees shall be required to adhere to a Code of Conduct and Acceptable Use Policy including maintaining confidentiality of Customer Data. Upon hiring and thereafter at least on an annual basis, employees shall receive regular security awareness training and must read and acknowledge Ardoq's information security policies.

3. Access Control

Customer data shall be processed in dedicated cloud-based production environments and limit access top such environments on a strict need to know basis for the purpose of delivering the Services. Administrative access shall be restricted to specifically authorized personnel, and access rights shall be reviewed on a regular basis. Multi-factor authentication (MFA) shall be required for access to production systems and most internal Ardoq business systems.

4. Operations Security

4.1 Ardoq shall implement cloud-native components to operate and secure the SaaS platform, including but not limited to containerisation, security groups and auto-scaling. Base virtual hosts shall be updated nightly with security patches. Containers shall be built on trusted base images and updated continuously as part of Ardoq's Continuous Delivery model.

4.2 Logs shall be aggregated from hosts and cloud infrastructure components and monitored using a SIEM. Logs will be retained for pre-defined periods based on business need and risk, in accordance with Ardoq retention policy.

5. Physical and Environmental Security

The Ardoq Cloud Platform shall be hosted with the cloud infrastructure providers listed in the applicable DPA (Hosting Providers). Customer acknowledges that physical and environmental security depends on Hosting Providers. Ardoq shall solely rely on Hosting Providers providing security compliance programs including certification against ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018 as

well as regular SOC 2 (Type II) audits. The audited security controls include dedicated security staff, strictly managed physical access control, and video surveillance.

6. Cryptography

6.1 Data in transit between Users and the Services shall be encrypted and authenticated using TLS 1.2.

6.2 Data at rest stored in the Ardoq Services shall be encrypted using 256-bit AES. Key management is supported by Hardware Security Modules (HSMs) validated under FIPS 140-2.

7. Communications Security

Ardoq shall monitor and mitigate against potential attacks by implementing tool such as, without limitation, a web application firewall, network-level firewalling, and security groups to segregate different processing operations. In addition, the Ardoq platform shall contain Distributed Denial of Service (DDoS) prevention defenses.

8. Software Development Lifecycle (SDLC) Security

8.1 Ardoq employs a Continuous Delivery model. Changes and improvements to the platform are developed and tested on separate branches and merged via Pull Requests. Pull Requests must be reviewed by at least one other developer for quality and security.

8.2 Third-party components shall be automatically reviewed for security vulnerabilities, triaged, prioritised, and updated.

8.3 The Ardoq Cloud Platform shall be subject to vulnerability assessments, including:

- Dynamic scans: Ardoq shall test for potential vulnerabilities on a weekly basis.
- Bug bounty program: Ardoq shall crowd-source vulnerability research through an invite-only bug bounty program.
- Annual penetration test: Ardoq shall contract an external third party to conduct an annual penetration test of the Cloud Platform to augment the other assessments.

9. Information Security Incident Management

Ardoq's security incident process flows and investigation data sources are pre-defined during recurring preparation activities and exercises, and are refined through investigation follow-ups. We use standard incident response process structures to ensure that the right steps are taken at the right time. Incident response exercises are conducted once per quarter.

10. Business Continuity Management

All Customer Data shall be backed up and stored in encrypted form at a separate cloud infrastructure provider. Production environments are instrumented using Infrastructure-as-Code technologies such as Terraform and Ansible, allowing for rapid re-deployment. Disaster response drills shall be conducted at least twice a year.

11. Compliance

11.1 Ardoq's ISMS shall maintain an ISO 27001:2017 certification. Ardoq’s ISMS implements a risk-based approach to planning, implementing, measuring and continuously improving appropriate

security controls. The scope of Ardoq's ISO 27001:2017 certification is the development, operation, and maintenance of the Ardoq SaaS platform.

11.2 Ardoq shall undergo annual SOC 2 (Type II) audits. The annual audit shall be based on the Auditing Standards Board of the American Institute of Certified Public Accountants' current Trust Services Criteria (AICPA TSC 2017). The audit report provides a third-party attestation of the organization's policies and processes relevant to security and may be provided upon request.

11.3 Ardoq is listed in the Cloud Security Alliance's Security, Trust, Assurance and Risk (STAR) registry. Customers and prospective customers can view our STAR Level 1 entry and access our completed CAIQ at https://cloudsecurityalliance.org/star/registry/ardoq/services/ardoq/.