FORESCOUT

Data Security Schedule for Customer Network Data in the Forescout Cloud Service

This Data Security Schedule ("**Schedule**") is incorporated by reference into Forescout's Data Processing Addendum ("**DPA**" or "**Agreement**") between Forescout and Customer available here: https://www.forescout.com/company/legal/. Capitalized terms used herein and not defined have the meaning ascribed to such terms in the Agreement including the Data Processing Addendum.

Any Personal Data that is provided to Forescout will be subject to the protections as set forth in the Agreement. The protections for Customer Network Data are as set below.

While handling Customer Data, Forescout will maintain a written information security program of policies, procedures and controls governing the processing, storage, transmission and security of Customer Data (the "**Security Program**"). The Security Program includes industry-standard practices designed to protect Customer Data from accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access. Forescout regularly tests, assesses and evaluates the effectiveness of the Security Program and may periodically review and update the Security Program to address new and evolving security technologies, changes to industry standard practices, and changing security threats, although no such update will materially reduce the commitments, protections or overall level of service provided to Customer as described herein.

1. DEFINITIONS

"**Customer Data**" means Customer Network Data and Personal Data.

"**Customer Network Data**" means the network traffic session information in the Customer's network collected, aggregated and processed by the Forescout Cloud Service. Customer Network Data does not include Forescout Data or Personal Data. Customer Data is considered Customer's Confidential Information and shall be protected in accordance with the terms of the Agreement.

"**Forescout Cloud Service**" mean the software applications that are provided as a cloud service by Forescout.

"**Forescout Data**" shall mean the data generated as a result of the classification and analysis by the Forescout Cloud Service. Forescout Data does not include Customer Data.

2. CUSTOMER NETWORK DATA

2.1 The data center hosting Customer Network Data will be compliant with the requirements as stated in the following standards: ISO9001:2015, ISO/IEC 27001:2013, ISO/IEC 27017:2015 and ISO/IEC 27018:2014 (or the then current substantially equivalent standards).

2.2 PHYSICAL SECURITY MEASURES.

(a) Access Restrictions. The data center facilities will have appropriate physical access restrictions and monitoring as well as fire detection and fire suppression systems. Physical access is controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.

(b) Power. The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility.

2.3 TECHNICAL SECURITY MEASURES.

(a) Access Administration. Access to the Customer Data by Authorized Persons is protected by authentication and authorization mechanisms. User authentication is required to gain access to the Forescout Cloud Service. Access privileges are based on the principles of "need to know" and "least privileges" and on job requirements and are revoked upon termination of employment or consulting relationships.

(b) Logging and Monitoring. The production infrastructure log activities are centrally collected and are secured to prevent tampering and are monitored for anomalies by a trained security team.

(c) Firewall System. An industry-standard firewall is installed and managed to protect Forescout systems by residing on the network to inspect all ingress connections routed to the Forescout Cloud Service.

(d) Vulnerability Management. Forescout conducts periodic independent security risk evaluations to identify critical information assets, assess threats to such assets, determine potential vulnerabilities, and provide for remediation. When software vulnerabilities are revealed and addressed by a vendor patch, Forescout will obtain the patch from the applicable vendor and apply it within an appropriate timeframe in accordance with Forescout's then current vulnerability management and security patch management standard operating procedure and only after such patch is tested and determined to be safe for installation in all production systems.

(e) Endpoint protection. Forescout updates endpoint protection software on regular intervals.

(f) Change Control. Forescout ensures that changes to platform, applications and production infrastructure are evaluated to minimize risk and are implemented following Forescout's standard operating procedure.

(g) Data Separation. Customer's cloud environment is identified by a unique client ID and deployment ID. Authentication in the upload and query ensures customers do not access one another's data.

(h) Encryption. Customer Network Data shall be encrypted in transit when it traverses from the Customer's Forescout appliance to the Forescout Cloud Service. Customer Network Data is encrypted at rest.

(i) Data Management. Each data center includes full redundancy (N+1) and fault tolerant infrastructure for electrical, cooling and network systems. The production database servers are replicated in near real time to a mirrored data center in a different geographic region.

(j) Data Backup. Customer Network Data that is created fewer than 90 days prior to the query data is accessible in the Forescout Cloud Service via a user interface. Customer Network Data will be stored in raw form for one (1) year, and then purged from the Forescout Cloud Service.

2.4 ADMINISTRATIVE SECURITY MEASURES.

(a) Personnel Security. Forescout performs background screening on Authorized Employees who have access to Customer Data in accordance with Forescout's then current applicable standard operating procedure and subject to applicable laws.

(b) Security Awareness and Training. Forescout maintains a security awareness program that includes appropriate training of Forescout personnel on the Security Program. Training is conducted at time of hire and annually throughout employment at Forescout.

(c) Vendor Risk Management. Forescout maintains a vendor risk management program that assesses all vendors that access, store, process or transmit Customer Data for appropriate security controls and business disciplines.

(d) Incident Monitoring and Management. Forescout will monitor, analyze and respond to security incidents in a timely manner in accordance with Forescout's standard operating procedure. Forescout's security group will escalate and engage response teams as may be necessary to address an incident.

(i) *Breach Notification*. Forescout will report to Customer any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data (a "**Breach**") without undue delay following determination by Forescout that a Breach has occurred.

(ii) *Report*. The initial report will be made to Customer security or privacy contact(s) designated in Forescout's customer support portal. As information is collected or otherwise becomes available, Forescout shall provide without undue delay any further information regarding the nature and consequences of the Breach to allow Customer to notify relevant parties, including affected Data Subjects, government agencies and data protection authorities in accordance with Data Protection Laws. The report will include the name and contact information of the Forescout contact from whom additional information may be obtained. Forescout shall inform Customer of the measures that it will adopt to mitigate the cause of the Breach and to prevent future Breaches.

(iii) *Customer Obligations*. Customer will maintain accurate contact information in the customer support portal and provide any information that is reasonably requested to resolve any security incident, including identify its root cause(s) and prevent a recurrence. Customer is solely responsible for determining whether to notify the relevant supervisory or regulatory authorities and impacted Data Subjects and for providing such notice.

(e) Penetration Tests.

(i) *By a Third Party*. Forescout contracts with third-party vendors to perform a penetration test on the Forescout Cloud Service twice a year to identify risks and remediation that help increase security. Upon a written request from Customer, Forescout will promptly provide to Customer a summary of the findings from the third-party vendor.

(ii) *By Forescout*. Forescout will conduct its own penetration test in accordance with its standard operating procedure.

3. USE OF AGGREGATE DATA.

Forescout may collect, use and disclose quantitative data derived from Customer's use of the Forescout Services for industry analysis, benchmarking, analytics, research, marketing, and other business purposes in support of the provision of the Forescout Services. Any such data will be in aggregate form only and such use will not disclose Customer Data. Forescout shall provide Customer with an election in the Forescout Services to participate in such use and if Customer chooses to not participate, then Forescout shall exclude Customer Data from such collection and analysis.

4. LIMITATIONS.

Notwithstanding anything to the contrary in this Schedule or other parts of the Agreement, Forescout's obligations extend only to those systems, networks, network devices, facilities and components over which Forescout exercises control. This Schedule does not apply to: (i) data in Customer's network or a third-party network or (ii) any data processed by Customer or its users in violation of the Agreement or this Schedule.

Customer agrees that it is solely responsible for its use of the Forescout Cloud Service, including securing its account authentication credentials (as applicable), and that Forescout has no obligation to protect Customer Network Data that Customer elects to store or transfer outside of Forescout's and Authorized Person's systems (e.g., offline or on-premises storage).