Last Revised: March 1, 2018

Citrix Services Security Exhibit

This Citrix Services Security Exhibit (the Exhibit) describes the technical and organizational security controls employed in connection with Citrix Cloud services, technical support services or consulting services under a Citrix license, subscription or services agreement. This Exhibit is incorporated by reference into such service agreements (the "Agreements"). This Exhibit does not apply to beta or lab/tech preview services, including Citrix Cloud Labs. Capitalized terms have the meaning stated in the Agreement or as defined herein, including Article 7, Definitions, below.

Article 1. Citrix Security Controls

This Article describes the physical, logical and administrative controls Citrix employs to secure the Services and Customer's associated security obligations. Citrix employs ISO/IEC 27002 as the baseline for its Services security program.

The controls specified in Article 1.A apply to all Services. The additional controls specified in Section 1.B apply to all generally available Citrix Cloud Services (collectively "Cloud Services").

Citrix reserves the right to modify the controls specified in this Article 1 provided that the controls employed during a term of service for which Customer has paid shall remain at least as protective of Customer Content as those specified in this Article 1 on the effective date of such term.

1.A. Enterprise Security Controls – All Services

Area	Control(s)
Security Program Management	**Security Ownership**. Citrix has appointed one or more security officers responsible for coordinating and monitoring the security controls for the Services. **Security Roles and Responsibilities**. Citrix personnel with access to Customer Content are subject to confidentiality obligations. **Service Security Policies.** Citrix maintains a comprehensive Global Security Framework (GSF), which provides the overarching security and safety principles established and approved by Citrix executive management. Policies provide security requirements in a clear and concise manner. Standards define the process or methodology of meeting policy requirements. The GSF security program undergoes regular reviews and evaluations. Citrix maintains a summary

Area	Control(s)
	of the GSF program and will provide it to customers upon request. **Product Risk Management.** Citrix performs assessments of key areas of risk associated with the Services including, by way of example only and as applicable, privacy risk assessments, open source reviews and export control analysis.
Asset Management	**Asset Inventory**. Citrix maintains an inventory of Citrix-managed equipment used to perform the Services ("Assets"). Identified system owners are responsible for maintaining and updating the inventory as needed. **Asset and Data Handling** Citrix identifies and classifies Customer Content to ensure access is appropriately restricted. Citrix imposes restrictions on printing Customer Content and disposing of printed materials that contain Customer Content. Citrix personnel must obtain authorization prior to storing Customer Content on portable devices, remotely accessing Customer Content, or processing Customer Content outside facilities managed by Citrix or its service providers.
Access Management	**Access Policy.** Citrix maintains a record of security privileges of individuals having access to Customer Content and follows the principle of least-privilege. **Access Authorization** Citrix maintains and updates a record of personnel authorized to access Citrix systems that contain Customer Content. New access to systems is reviewed and approved by management prior to being granted. Citrix performs regular reviews of user accounts and assigned permissions for key systems. Citrix identifies those personnel who may grant, alter or cancel authorized access to data and resources. Citrix ensures that where more than one individual has access to systems containing Customer Content, the individuals have separate identifiers/log-ins.

Area	Control(s)
	Least-Privilege Citrix restricts access to Customer Content to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** Citrix requires that users secure computers and data while unattended. Citrix requires that passwords remain unintelligible throughout their lifecycle. **Authentication** Citrix uses industry-standard practices to identify and authenticate users accessing information systems. Where authentication mechanisms are based on passwords, Citrix follows industry-standard practices for password handling and management, including: Passwords are renewed regularly, as dictated by system requirements and Citrix standards Passwords must meet length and complexity requirements, including a minimum length of 8 characters Personnel are prohibited from sharing passwords De-activated or expired identifiers are not granted to other individuals Citrix maintains procedures to deactivate passwords that have been corrupted or inadvertently disclosed. Citrix monitors repeated attempts to gain access to the Services using an invalid password. Citrix uses practices designed to maintain the confidentiality and integrity of passwords when they are assigned, distributed and stored.
Loss Prevention	**Malicious Software**. Citrix uses anti-virus software and other controls to avoid malicious software gaining unauthorized access to Customer Content, including malicious software originating from public networks. **Media Disposal.** Citrix disposes of media when no longer required based on classification and

Area	Control(s)
	using secure deletion processes.
Physical and Environmental Security (Access Control, Availability Control)	**Physical Access to Citrix Facilities**. Citrix limits facilities access to authorized individuals. ID badges are required for employees, contractors and guests and must be visible at all times when in the facility. Citrix monitors facility entry points using various methods including security guards, intrusion detection and CCTV cameras. **Protection from Disruptions**. Citrix uses systems to protect against loss of data due to power supply failure or line interference, including global and redundant service infrastructure that is set up with disaster recovery sites; evaluating data centers and Internet service providers (ISPs) to optimize performance regarding bandwidth, latency and disaster recovery isolation; situating data centers in secure facilities that are ISP carrier neutral and provide physical security, redundant power, and infrastructure redundancy; and uptime agreements from key suppliers. **Hosted Data Centers.** When Citrix uses third-party co-located data centers for provision of the Services, Citrix requires that the service provider meets or exceeds the physical and environmental security requirements of Citrix-managed facilities. Minimum security requirements include, but are not limited to: • Physical access restrictions and safeguards (authentication, logs, monitoring, etc.) • Adequate separation of environments • Fire suppression, detection, and prevention mechanisms • Climate control systems (temperature, humidity, etc.) **Cloud Computing.** When Citrix uses XaaS [Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS)] for provision of the Services, Citrix contracts with XaaS providers that provide a materially similar level of physical access control to its hosted data centers.
Application and Development Security	**System Development & Maintenance.** Citrix maintains a Secure by Design process, which includes standards and change control procedures designed to address security requirements of information systems, code review & testing, and security around the use of test data. This process is managed and monitored by a specialized security engineering team, which is also

Area	Control(s)
	responsible for design review, threat modeling, manual code review & spot checks, and penetration testing. **Open Source Management**. Citrix uses a software-based system for managing open source reviews and approvals. In addition, Citrix conducts periodic scans and audits of its software products to confirm open source compliance. **Change Management.** Citrix maintains change control procedures that address security requirements of information systems, testing, acceptance of testing, and security around the use of test data. Software and configuration changes are managed and tracked using standard ticketing systems.
Secure Operations	**Network Design**. Citrix implements mechanisms designed to enforce access management policies and standards across the Services, including network controls over access to Customer Content. These include, as appropriate: configuring an intermediate untrusted zone between the Internet and the internal network that includes a security mechanism to restrict access and unauthorized traffic; and separating web and application servers from the corresponding database servers in a tiered structure that restricts traffic between the tiers.
Incident Management	**Incident Response**. Citrix maintains an incident response program designed to contain, analyze, remediate and communicate security and safety incidents impacting Citrix managed networks and/or systems or Customer Content. **Incident Notification**. If Citrix determines that Customer Content within its control has been subject to a Security Incident, Customer will be notified within the time period required by applicable law. **Incident Recording**. Citrix maintains a record of known Security Incidents with a description of the incident, the time period, the consequences of the incident, the name of the reporter, to whom the incident was reported, and the procedure for recovering data and Services as applicable.
Vendor Management	**Onboarding**. Citrix performs security assessments of service providers that will have access to

Area	Control(s)
	Customer Content and/or to components of the Services that process Customer Content. Citrix requires service providers connected with the Services to comply with the level of security in this Section applicable to the services they provide. Service providers that may access Customer Content subject to European Union law are required to self-certify to EU-U.S. and EU-Swiss Privacy Shield programs or to execute Standard Contractual Clauses. **Ongoing Maintenance.** Service providers are assessed periodically, based upon the sensitivity and risk associated with their services. **Off-boarding.** Upon termination of a supplier relationship, the service provider is required to return all Customer Content in its possession or to certify that all Customer Content has been securely destroyed.
Business Continuity and Disaster Recovery	**Business Continuity.** Citrix maintains emergency and contingency plans for the facilities in which Citrix information systems that process Customer Content are located. **Disaster Recovery.** Citrix's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Content in its original or last-replicated state.
Customer Security Obligations	Customer is responsible for managing security not expressly included as part of the Services. This includes, but is not limited to: • Limiting Citrix's access to Customer Content only to what is needed for Customer to receive the Services. • Protecting its network and service components against interference, including monitoring and securing its networks and computing equipment. • Downloading Customer Content where needed, both during the term of Services and upon termination. • Citrix either encrypts data in transit by default or offers customers means to encrypt data in transit. Further detail is provided in the product documentation for the Services. Customer is responsible for ensuring that data is appropriately secured in transit.

1.B. Additional Cloud Services Security Controls

Area	Control(s)
Data Protection (Availability Control, Transmission Control, Data Deletion)	**Failover Procedures**. Citrix implements mechanisms designed to address loss of availability of Customer Content, including storing copies of Customer Content in a different place from where the primary computer equipment processing the Customer Content is located. **Data Beyond Boundaries**. Citrix encrypts or enables Customer to encrypt Customer Content that is transmitted over public networks that are part of a Service. **Retention.** Citrix may retain Customer Content following the Service period and archiving for customer access where required for legal purposes. Citrix will comply with the requirements of this Exhibit until such Customer Content has been permanently deleted. Subject to Return directly below, Citrix is under no obligation to retain Customer Content following termination of the Service. **Return.** Subject to availability and the applicable Services Description, Customer has thirty (30) days to download Customer Content after expiration. **Data Deletion**. Citrix will securely delete Customer Content when no longer needed for a legitimate purpose.
Secure Operations	**Event Logging**. In certain Services, Citrix collects Logs. Logs may include access ID, time, authorization granted or denied, diagnostic data such as trace and crash files, and other relevant activity. Logs are used (**i**) for providing, securing, managing, measuring and improving the Services and associated analytics, (**ii**) as directed or instructed by Customer and its Users, and/or (**iii**) for compliance with Citrix policies, applicable law, regulation, or governmental request. This may include monitoring the performance, stability, usage and security of the Services and related components. Customer may not block or interfere with this monitoring. Citrix may supplement Logs with information collected from third parties for the purposes specified above. Logs may be used for purposes not specified in this Exhibit only in aggregate form.
Business Continuity and Disaster Recovery	**Back-ups.** Except where otherwise noted in the respective Services Description, Services are maintained in high availability, active-active clusters spanning multiple physical sites. Systems not maintained in an active-active configuration are backed up according to the specific Service's Service Level Goals.

Area	Control(s)

Article 2. Treatment of Personal Data

Personal data is information about an identified or identifiable individual. Customer determines the personal data that it includes in Customer Content. In performing the Services, Citrix acts as a data processor and Customer remains the data controller for any personal data contained in Customer Content. Citrix will act on Customer's instructions regarding the processing of such personal data, as specified in the Agreement.

Further information concerning the treatment of personal data subject to the General Data Protection Regulation, including the mechanisms employed for international transfer of such data, is provided in Exhibit I, General Data Protection Regulation Terms.

Article 3. Location of Services

Customer Content may be transferred to, stored and/or processed in the United States or in other countries where Citrix and/or its service providers operate. The requirements of this Exhibit continue to apply, regardless of where Citrix stores or processes Customer Content.

The parties may negotiate in good faith regarding any further data processing or data transfer agreements needed to facilitate the lawful transfer of data internationally in connection with Citrix's provision of the Services.

Article 4. Disclosure of Customer Content

Customer consents to Citrix's disclosure of Customer Content as set forth in this section.
Citrix may use subcontractors and agents to perform Services. Any subcontractors and agents shall be entitled to access Customer Content only as needed to perform the Services and shall be bound by written agreements that require them to provide at least the level of data protection required of Citrix by this Exhibit, as applicable. Citrix remains responsible at all times for its subcontractors' and agents' compliance with the terms of the Agreement, as applicable.

Citrix also may disclose Customer Content to (a) affiliated entities, for purposes consistent with the Agreement; (b) in connection with any anticipated or actual merger, acquisition, sale, bankruptcy or other reorganization of some or all of its business, subject to the obligation to protect Customer Content consistent with the terms of the Agreement; or (c) for legal purposes, including enforcement of its rights, detecting and preventing fraud, protecting against harm to the rights or property of Citrix, Customers, Users, or the public; and (c) as required by law, including in response to a subpoena, judicial or administrative order, or other binding instrument (each a "Demand"). Except where prohibited by law, Citrix will promptly notify Customer of any Demand and provide Customer assistance reasonably necessary for Customer to respond to the Demand in a timely manner.

Article 5. Customer Obligations

1. General. Customer may use and access the Services only as permitted by the Agreement. Customer will comply with all laws applicable to it in connection with its use of the Services.

2. Permissions. Customer is responsible for obtaining all permissions necessary for Citrix to perform the Services, including providing any notices and obtaining any consents or licenses needed for Citrix to access and process the Customer Content as set forth in this Exhibit.

3. Regulatory. Customer is responsible for determining whether any Customer Content is subject to additional regulatory or security requirements beyond those specified in the Agreement, including this Exhibit. Customer shall not submit or store any Customer Content that is governed by US International Traffic in Arms Regulations (ITAR) or similar regulations of any country that restricts import or export of defense articles or defense services. Further, Customer shall not provide or store any Customer Content subject to additional regulatory requirements, such as protected health information ("PHI"), payment card information ("PCI"), or controlled-distribution data under government regulations, unless specified in the Customer's Order and applicable Service Description and the parties have entered into any additional agreements (such as a Business Associate Agreement (BAA)) in advance as may be required for Citrix to process such data. Customers of the ShareFile service may contact Citrix at privacy@sharefile.com to request a BAA.

4. Customer Security Environment. The Services are designed to be delivered only within a larger Customer security environment. Customer shall ensure appropriate security functionality for all components not expressly managed by Citrix including, but not limited to, access controls, firewalls, applications and networks used in conjunction with the Services. See Section 1.A., Customer Security Obligations, above.

5. Security Notification. Customer is responsible for notifying Citrix promptly of any security incidents involving the Services and/or Customer Content as outlined in Article VI, Citrix Contacts, below.

6. User Compliance. Customer is responsible for its Users' compliance with the terms of the Order and the Agreement.

Article 6. Citrix Contacts

FUNCTION	CONTACT
Customer Support	https://www.citrix.com/contact/technical-support.html
Reporting an Incident	secure@citrix.com
Suspected vulnerabilities in Citrix products	secure@citrix.com

Article 7. Definitions

Capitalized terms in the Exhibit shall have the meaning specified in the Agreement or below. In the event of a conflict between the remaining terms of the Agreement and any definition below, the definition below shall apply to this Exhibit.

Customer Content means any data uploaded to Customer's account for storage or data in Customer's computing environment to which Citrix is provided access in order to perform Services.

Log means a record of events related to the Services, including records that measure performance, stability, usage, security, and support.

Security Incident means unauthorized access to Customer Content resulting in the loss of confidentiality, integrity or availability.