
citrix.

Citrix Services Security Exhibit

Version 2.0
Effective April 20, 2020

Contents

Scope.....	3
Security Program and Policy Framework.....	3
Access Control	4
System Development and Maintenance.....	5
Asset Management.....	5
Human Resources Security	6
Operations Security	7
Physical Security.....	8
Business Continuity & Disaster Recovery	9
Incident Response	9
Vendor Management.....	10
Compliance	10
Customer Audits and Inquiries	11
Citrix Contacts.....	12

This Citrix Services Security Exhibit (the “Exhibit”) describes the security controls implemented in connection with the performance of Citrix Cloud services, technical support services or consulting services (the “Services”) delivered to customers under the relevant Citrix license and/or services agreement and the applicable order for the Services (collectively, the “Agreement”). Beta or lab/tech preview services (including Citrix Cloud Labs) and internal Citrix IT systems not involved in the delivery of Services are outside of the scope of this Exhibit.

Capitalized terms have the meaning stated in the Agreement or as defined herein. “Customer Content” means any data uploaded to Customer’s account for storage or data in Customer’s computing environment to which Citrix may be provided access to in order to perform Services. “Logs” means records of Services, including, but not limited to, data and information on performance, stability, usage, security, support, and technical information about devices, systems, related software, services or peripherals associated with Customer’s use of Services.

1. Scope

This Exhibit describes the administrative, physical and technical security controls Citrix employs in order to maintain the confidentiality, integrity and availability of its Services. These controls apply to Citrix’s operational and Services systems and environments. Citrix employs ISO/IEC 27002 as the baseline for its Services security program.

Citrix seeks to continually strengthen and improve its security practices, and so reserves the right to modify the controls described herein. Any modifications will not diminish the level of security during the relevant term of Services.

2. Security Program and Policy Framework

Citrix has a security program and policy framework that is established and approved by Citrix senior and executive management representing various business areas throughout the company.

2.1 Security Risk Oversight

The Citrix Cyber Risk Oversight Committee (CROC) governs security risk management activities. The CROC consists of cross-functional management and leadership. The executive leadership team reviews committee membership on an annual basis to confirm adequate coverage of business and operational areas.

The CROC meets at least quarterly and provides guidance, insight, and direction in identifying, assessing and addressing security risks in both corporate operations as well as service delivery infrastructure.

2.2 Security Risk Management

Citrix utilizes a security risk management (SRM) program that identifies potential threats to Citrix products and services and to Citrix infrastructure, rates the significance of the risks associated with those threats, develops risk mitigation strategies, and partners with Citrix’s Product and Engineering teams to implement those strategies.

The SRM program applies industry-recognized frameworks, such as ISO/IEC 31000 and ISO/IEC 27005.

2.3 Information Security

Citrix has appointed a Chief Information Security Officer (CISO), who is responsible for security oversight and policy strategy, compliance and enforcement. The Director of Security Monitoring and Response leads the incident response process, including investigation, containment and remediation.

2.4 Physical and Environmental Security

The Citrix Security team, together with Facility Management, oversees the physical access to Citrix facilities.

3. Access Control

Citrix requires the use of access control measures designed to ensure appropriate privileges are assigned and maintained for access to company systems, assets, data and facilities in order to protect against potential damage, compromise, or loss. Citrix follows the Least Privilege Principle, or role-based security, limiting user's access to only what is necessary to perform job functions or roles.

Managers design roles to provide adequate segregation of duties, distributing tasks and privileges among multiple people in order to safeguard against fraud and error.

3.1 New Accounts, Roles, and Access Requests

Citrix requires a formal request for access to company systems or data. Each access request requires a minimum approval of the user's manager to confirm the user's role requires access. Access administrators confirm that necessary approvals are obtained prior to granting access to systems or data.

3.2 Account Review

Citrix maintains and updates a record of security privileges for employees and contractors authorized to access Citrix systems containing Customer Content. The principle of least-privilege is applied.

Citrix performs, at minimum, bi-annual reviews of user accounts and assigned permissions for key systems. Any changes required as a result of the reviews are subject to a formal access request process to confirm the user and the user's role requires access to the relevant system(s).

3.3 Account, Role, and Access Removal

Citrix requires user access be disabled, revoked, or removed promptly upon notification of a user's role change (if applicable), termination, user's conclusion of engagement, or departure from the company.

Access removal requests are documented and tracked.

3.4 Credentials

Citrix requires multi-factor authentication for remote access to Citrix systems by employees, and enforces the following password handling and management practices:

- Passwords are renewed regularly, as dictated by system requirements set by Citrix
- Passwords must meet length and complexity requirements, including a minimum length of 10 characters and not allowing common or dictionary words

-
- De-activated or expired user IDs are not granted to other individuals
 - Citrix maintains procedures to deactivate passwords that have been inadvertently disclosed
 - Citrix monitors repeated attempts to gain access to the Services using an invalid password and takes automated actions to block repeated attempts

Citrix uses practices designed to maintain the confidentiality and integrity of passwords when they are assigned, distributed and stored, such as:

- Citrix requires that passwords remain hashed throughout their lifecycle
- Citrix prohibits the sharing of passwords

4. System Development and Maintenance

Citrix maintains a Secure by Design process, which includes standards and change controls procedures designed to address security requirements of the information systems, code review and testing, and security around the use of test data. This process is managed and monitored by a specialized security team, which is also responsible for designed review, threat modeling, manual code review and spot checks, and penetration testing.

4.1 Secure Design Principles

Citrix has adopted a formal systems development life cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology requirements.

Citrix uses a software-based system for managing open source reviews and approvals, which includes conducting periodic scans and audits of its software products. Citrix has documented policies, available to all employees, regarding the use of Open Source as well as training for developers and their management on Open Source best practices.

4.2 Change Management

The Citrix infrastructure and software change management process addresses security requirements and requires that software and infrastructure changes to be authorized, formally documented, tested (as applicable), reviewed, and approved prior to migration to the production environment. Infrastructure and software changes are managed and tracked using work management systems.

The change management process is appropriately segregated, and access to migrate changes to production is restricted to authorized personnel.

5. Asset Management

5.1 Physical and Virtual Asset Management

Citrix maintains a dynamic inventory of Citrix-managed physical and virtual systems used to perform the Services (“Service Assets”). System owners are responsible for maintaining and updating their Service Assets consistent with Citrix security standards.

Formal disposal procedures are in place to guide the secure disposal of Citrix and Customer data. Citrix disposes of data when no longer required based on classification and using deletion processes designed to prevent data from being reconstructed or read.

Citrix technology assets are sanitized and disposed when they are no longer needed within their designated or assigned area. Technology assets include but are not limited to individual computing devices, multifunction computing devices, imaging devices, and network appliances. Disposal is coordinated through Global Security Risk Services and Information Security.

5.2 Application and System Management

Application and system owners are responsible for reviewing and classifying the data they store, access, dispose of, or transmit. Among other controls, employees and contractors are required to:

- Classify Customer Content as among the highest two categories of Citrix confidential information, and apply appropriate access restrictions
- Restrict the printing of Customer Content and dispose of printed materials in secure containers
- Not store corporate or Confidential Information on any equipment or device that does not meet the requirements of Citrix security policies and standards
- Secure computers and data while unattended

5.3 Data Retention

Customer Content stored as part of Citrix Cloud services is accessible by the Customer for a limited time period following the termination of Services and then deleted (except for back-up copies) after confirmation has been sent to Customer that deletion will occur. Additional details are provided in the specific services documentation. Customer Content may also be retained following the completion of the services if required for legal purposes. Citrix will comply with the requirements of this Exhibit until such Customer Content has been permanently deleted.

6. Human Resources Security

Maintaining the security of Customer Content is one of the core requirements for all Citrix employees and contractors. Citrix's Code of Business Conduct requires all employees and contractors to adhere to Citrix security policies and standards, and specifically addresses the protection of confidential information as well as personal information of Citrix Customers, partners, suppliers and employees.

All Citrix employees and contractors are subject to confidentiality agreements that cover Customer information. The Citrix Security organization also regularly communicates to employees on topics related to information and physical security in order to maintain security awareness on specific topics.

6.1 Background Screening

Citrix currently uses background screening vendors for all new hires globally and requires the same for its third party supplier personnel, except where limited by local law or employment regulations.

6.2 Training

All employees are required to take training on data protection and on company policies designed to protect the security of Citrix Confidential Information, which includes the Confidential Information of our Customers, partners, suppliers and employees. The training covers privacy practices and the principles that apply to employee handling of personal information, including the need to place limitations on using, accessing, sharing and retaining personal information. Members of the Engineering organization undergo specific training that consists of secure development, architecture, and coding.

6.3 Enforcement

All employees are required to comply with Citrix security and privacy policies and standards. Noncompliance is subject to disciplinary action, up to and including termination of employment.

7. Operations Security

7.1 Network and System Security

Citrix has documented network and system hardening standards designed to ensure that networks and systems are securely configured. Required procedures under these standards include, but are not limited to:

- Changing or disabling default settings and/or accounts
- Applying login banners
- Controlled use of administrative access
- Restrict service accounts for only the purpose which they were created
- Configure logging and alert settings appropriate for auditing

Citrix requires the implementation of anti-malware software on servers and workstations, and scans the network for malicious software.

Network controls govern access to Customer Content. These include, as applicable: configuring an intermediate untrusted zone between the Internet and the internal network that includes a security mechanism to restrict access and unauthorized traffic; network segmentation to prevent unauthorized access of Customer Content; and separating web and application servers from the corresponding database servers in a tiered structure that restricts traffic between the tiers.

7.2 Logging

Citrix collects Logs to confirm the correct functioning of our Services, to assist with troubleshooting system issues and to protect and secure our networks and Customer Content. Logs may include access ID, time, authorization granted or denied, diagnostic data such as trace and crash files, and other relevant information and activity.

Logs may be used in an identifiable form (i) for providing, securing, managing, measuring and improving the Services and associated analytics, (ii) as requested by Customer or its end-users, and/or (iii) for compliance with Citrix policies, applicable law, regulation or government request. This may include monitoring the performance, stability, usage and security of the Services and related components. Customers may not block or interfere with this monitoring.

For more information on Customer Content and Log handling, please see the Citrix Trust Center [Privacy & Compliance section](#), which contains several white papers on Citrix Logging.

7.3 Protection of Data in Transit

Citrix has deployed secure transmission protocols for transmission of information over public networks that are part of the Services. The Services are protected by encryption and access via the internet is protected by TLS connections.

8. Physical Security

8.1 Citrix Facilities

Citrix maintains the following controls designed to prevent unauthorized access to any facility:

- Facility access is limited to authorized individuals
- Visitors are required to register in a digital visitor log and be escorted or observed at all times
- ID badges are required for employees, contractors, and guests and must be visible at all times when in the facility
- Security manages and controls after-hours access to facilities
- Security guards, intrusion detection, and/or CCTV cameras monitor building entry points, loading and shipping docks, and public access areas – (mechanisms for monitoring access may differ between facilities, depending on the facility and location)

In addition, Citrix facilities provide:

- Fire suppression and fire detection systems or devices
- Climate control systems or devices (temperature, humidity, etc.)
- Accessible water master shutoff or isolation valves
- Alternate power sources (generator, UPS system, etc.)
- Emergency exits and evacuation routes

Data closets located in offices are protected via badge access and monitoring.

8.2 Data Centers

In addition to the Citrix facilities controls described above, for Citrix-owned and managed facilities, Citrix implements additional controls at the data centers it uses to provide Services.

Citrix uses systems designed 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. Data centers and Internet service providers (ISPs) are evaluated to optimize performance regarding bandwidth, latency and disaster recovery isolation.

Data centers are situated in facilities that are ISP carrier neutral and provide physical security, redundant power, infrastructure redundancy and uptime agreements from key suppliers.

When Citrix uses third-party data centers or cloud services for the delivery of the Services, Citrix contracts providers that meet or exceed the physical and environmental security requirements of Citrix facilities.

9. Business Continuity & Disaster Recovery

9.1 Business Continuity

Citrix strategically plans for the continuation of business operations during adverse or disruptive situations, and designs systems to keep the services operational during the occurrence of such events.

Citrix performs a department-level Business Impact Analysis (BIA) at least every two years, with an annual review each year. The BIA is used to create a departmental Business Continuity Plan (BCP), which identifies and documents for each department its resource requirements, recovery parameters and methods, relocation needs, and the security safeguards required throughout the process to avoid failures or gaps. Senior management of each department reviews and approves the BCP on an annual basis, or as significant organizational changes occur.

Citrix maintains emergency and contingency plans for all Citrix facilities. In the event facilities are not available, employees have the option to work remotely either at other Citrix facilities or the location of their choosing. Additional recovery strategies are documented in the BCPs where applicable.

9.2 Disaster Recovery

Citrix endeavors to minimize the impact of service or operational disruptions by implementing processes and controls designed to ensure stable and orderly restoration and recovery of Citrix business systems and data. Citrix implements redundancy for all mission-critical systems, data, and infrastructure. The Disaster Recovery Plan (DRP) uses the assessment performed in the BIA mentioned above to identify and document recovery time parameters, methods, priorities, and security safeguards required throughout the process to avoid failures or gaps.

The plan outlines the overall structure and approach to restoring critical systems and data, including but not limited to:

- Roles and responsibilities of individuals or teams
- Contact information for essential personnel or third-parties
- Training requirements and plans for essential personnel
- Recovery objectives, restoration priorities, and success metrics
- Schema of full recovery and restoration

Senior management reviews and approves the DRP on an annual basis, or as significant organizational changes occur.

10. Incident Response

Citrix maintains a Cyber Security Incident Response Plan that details the processes for detecting, reporting, identifying, analyzing, and responding to Security Incidents impacting Citrix managed networks and/or systems or Customer Content. Security Incident response training, and testing takes place at least annually.

“Security Incident” means unauthorized access to Customer Content resulting in the loss of confidentiality, integrity or availability. 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 law. Citrix’s notice will describe, where known, the nature of the incident, the time period, and the potential impact to the Customer.

Citrix maintains a record of each Security Incident.

11. Vendor Management

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. A list of Citrix subprocessors that may have access to Customer Content is available on the [Citrix Trust Center](#).

11.1 Onboarding

Citrix’s Third Party Risk Management Program provides a systematic approach to managing security risks posed by the use of third party suppliers. Citrix works to identify, analyze and mitigate security risks prior to engaging in the procurement of such third parties.

Citrix executes agreements with suppliers to document relevant security measures and obligations consistent with those specified in this Exhibit.

11.2 Ongoing Assessment

Citrix performs periodic security risk assessments designed to ensure security measures remain in place throughout the supplier relationship. Changes to services provided or changes to existing contracts require a security risk assessment to confirm that the changes do not present additional or undue risk.

11.3 Off-boarding

Citrix notifies the company’s procurement organization 90 days prior to the plan to end a supplier relationship or prior to a contract expiration with a supplier. The company’s procurement organization coordinates the termination of the existing relationships to confirm that Citrix corporate data and assets are secured and properly handled.

12. Compliance

12.1 Treatment of Personal Data

Personal data is information that relates to 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 Citrix’s Data Processing Agreement.

12.2 Location of Services

Citrix Cloud Services Customers retain control over the choice of geographic location of their Cloud Services environment (see also [Citrix Cloud Geographical Considerations](#)). At no point during the applicable Cloud Services subscription will Citrix change the geographical location of the environment chosen by Customer without Customer's consent. Note that as part of general Service delivery, Customer Content may be transferred to the United States or other countries where Citrix and/or its service providers operate as necessary to provide the Services.

12.3 Disclosure of Customer Content

Citrix may disclose Customer Content to the extent 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.

12.4 Customer Security and Regulatory Requirements

The Services are designed to be delivered within a larger Customer IT environment, and so Customers retain full responsibility for all aspects of security not expressly managed by Citrix including, but not limited to, access controls, firewalls, applications and networks that Customers may use in conjunction with the Services.

Customers remain responsible for determining whether their use of Services, including providing Citrix with access to any Customer Content as part of the services, is subject to regulatory or security requirements beyond those specified in the Agreement, including this Exhibit. Customers must therefore ensure that they do not submit or store any Customer Content that is governed by laws that impose specific controls that are not included in this Exhibit, which may include US International Traffic in Arms Regulations (ITAR) or similar regulations of any country that restricts import or export of defense articles or defense services, protected health information ("PHI"), payment card information ("PCI"), or controlled-distribution data under government regulations, unless specified in the Agreement and applicable Service Description and the parties have entered into any additional agreements (such as a HIPAA Business Associate Agreement) in advance as may be required for Citrix to process such data.

13. Customer Audits and Inquiries

Up to once annually, Citrix will respond to audit requests in the form of responses to Customer risk assessments. Customers may also access the Citrix Due Diligence package at any time for an updated security package and questionnaire. The Citrix Security Due Diligence Package was created for customer security inquiries and provides readily available security information. The Citrix Due Diligence Package includes three documents for each product: a completed 300+ question Shared Assessments' Standardized Information Gathering (SIG) Lite questionnaire, an overview of Citrix's security posture and controls, and an evidence package of selected policies and controls. The SIG questionnaire is the most used questionnaire among our Customers and is leveraged across all industry sectors. The Due Diligence Package can be downloaded from the [Citrix Trust Center](#).

14. Citrix Contacts

Function	Contact
Customer Support	https://www.citrix.com/contact/technical-support.html
Reporting a Security Incident	secure@citrix.com
Suspected vulnerabilities in Citrix products	https://www.citrix.com/about/trust-center/security.html#lightbox-38764 (Click the "Report a Security Issue" button.)



Enterprise Sales

North America | 800-424-8749

Worldwide | +1 408-790-8000

Locations

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States

Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

©2020 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).