# CITRIX SUPPLIER SECURITY STANDARDS

These Supplier Information and Physical Security Standards (the "Standards") list the technical and organizational measures and security controls that Citrix's Vendors and Partners (for purposes of this document, collectively referred to as "Suppliers") are required to adopt when (a) accessing Citrix or Citrix customer Facilities, Networks and/or Information Systems, or (b) accessing, processing, or storing Citrix Confidential Information.

Supplier is responsible for compliance with these Standards by its Personnel, including ensuring that all Personnel are bound by contractual terms consistent with the requirements of these Standards. Additional security compliance requirements may be specified in Supplier's Agreement or individual statement of work.

The Standards contain the following sections:



## Section 1: Personnel/Human Resources (HR) Security

1.1 Supplier must perform Criminal and employment background checks, consistent with local laws and regulations, for all Personnel. The level of verification performed must be proportional to risk correlated to roles within the organization.

1.2 Supplier Personnel are required to agree, in writing, to abide by Supplier's security requirements and organizational policies.

1.3 Supplier must have a comprehensive security awareness program for all Personnel that encompasses education, training and updates for security policies, procedures and requirements. Training must be provided at time of hiring and repeated at regular intervals thereafter (no less than every two years, and more frequently to the extent required by applicable law, regulation or standard (such as FedRAMP)).

1.4 Supplier must have formal disciplinary processes in place for Personnel and take appropriate action against Personnel who violate Supplier's organizational policies, based upon the nature and gravity of the violation.

1.5 Upon termination of Personnel employment, Supplier must promptly remove access to Information Systems, Networks and Applications and confirm Personnel have not retained any Confidential Information.

1.6 Supplier is authorized to use subcontractors for the provision of the Services as long as Supplier is responsible for and contractually binds any subcontractor to comply with nondisclosure terms and security standards consistent with those set forth in the Agreement and this document.

1.7 Supplier must maintain and regularly update a list specifying its subcontractors, the country of destination of the data, and provide that list to Citrix upon reasonable notice. Citrix reserves the right to reject the use of any subcontractor, or require reasonable steps to address objections to a subcontractor, for justified reasons.

## Section 2: Information Security Organization, Policy and Procedures

2.1 Supplier must have clearly defined organizational information security roles, responsibilities and accountability.

2.2 Supplier must publish, maintain and enforce formal written information security policies. Information security policies must be approved by management and communicated to Personnel. Personnel must be made aware of their obligations to protect Confidential Information, as well as the acceptable use of all Networks, Information Systems and Computers. The information security policies must be reviewed every year and updated as necessary.

2.3 Supplier must classify and label Information and enforce role-based access in accordance with their information classification scheme and in terms of its sensitivity.

2.4 Supplier must implement security processes for managing its suppliers involved in the delivery of Services, which shall include a process for confirming their ability to meet the applicable security controls set forth in these Standards.

2.5 Supplier must maintain an inventory of assets that includes all business-critical Information Systems and information processing sites used in the delivery of Services to Citrix. The inventory must be accurate, remain current and include owners responsible for each asset.

2.6 Supplier must maintain an up to date record of Personnel who have access to Facilities, Information Systems, Networks and Applications, including their geographic location. Personnel access must be reviewed at least bi-annually and access promptly revoked when no longer deemed necessary for job function.

## Section 3: Compliance and Assessments

### 3.1 Regulatory Compliance

3.1.1 If Services involve Payment Card Information (PCI), Supplier will maintain compliance with the current version of the Data Security Standards (DSS) from the Payment Card Industry Security Standards Council (PCI SSC) for the duration of the Services provided to Citrix. On request, Supplier must provide Citrix the most recent PCI SSC “Attestation of Compliance” (AoC) reports prepared by a third party PCI Qualified Security Assessor (QSA) for both Supplier's systems and for any third-parties used by the Supplier for handling payment card data.

3.1.2 If Services involve Protected Health Information (PHI) subject to the U.S. Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated under that Act (collectively, HIPAA), the Supplier will maintain compliance with HIPAA. On request, Supplier must provide Citrix reasonable assurance that Supplier (and any third-parties used by the Supplier for handling PHI) maintains sufficient technical and organizational controls to comply with HIPAA requirements. This assurance may include audits and assessments from a qualified third-party and/or completion of a questionnaire with sufficient evidence to support Supplier’s compliance.

3.1.3 Supplier must inform Citrix if legislation applicable to the Supplier could prevent the Supplier from fulfilling the obligations relating to treatment of Citrix Personal Information.

3.1.4 In the event Supplier processes Confidential Information that is subject to additional regulatory requirements, or in a manner subject to additional regulatory requirements, Supplier agrees to cooperate with Company to comply with such requirements, including negotiating in good faith additional agreements as required for such compliance.

3.1.5 Supplier will comply with its obligations under applicable data protection laws. In the event Supplier

processes Personal Information, Citrix and the Supplier must sign a data processing agreement.

### 3.2 Security Compliance

3.2.1 Suppliers accessing Citrix's Network may be required to execute a Citrix network access agreement.

3.2.2 Upon request, Supplier must confirm, in writing, the Supplier's compliance with the requirements of these Standards and provide written responses to any questions that Citrix presents to Supplier regarding its security practices.

### 3.3 Security Assessments

3.3.1 Citrix reserves the right to perform security assessments to verify compliance with these Standards. Citrix will provide reasonable notification of a verification audit, ensure the audit is performed during normal business hours, and with minimal disruption to the Supplier's business operations.

3.3.2 Supplier must promptly correct any material noncompliance issues identified during the security assessment.

3.3.3 Supplier cloud-based services provided to Citrix must undergo a penetration testing by an independent 3rd party, and summary findings made available to Citrix upon request. Any finding during the assessment must be remediated.

## Section 4: Security Incident Management and Reporting

4.1 Supplier must have documented information Security Incident procedures, enabling effective and orderly management of Security Incidents. The procedures must cover the reporting, analysis, monitoring and resolution of Security Incidents.

4.2 Reported Security Incidents must be verified and then analyzed to determine their impact. All confirmed Security Incidents must be classified, prioritized and documented.

4.3 Security Incidents must be handled by a dedicated Security Incident response team or Personnel who are trained in handling and assessing Security Incidents in order to ensure appropriate procedures are followed for the identification, collection, acquisition and preservation of information.

4.4 Supplier must report Security Incidents relating to the Citrix Services and/or Confidential Information within 72 hours of confirmation. Security Incidents must be reported to **secure@citrix.com.**

4.5 Unless otherwise required by law or law enforcement, Supplier must not make any statements concerning a security incident identifying or concerning Citrix without written authorization of Citrix's Legal Department.

4.6 Unless prohibited by law, Supplier must promptly notify Citrix in the event the Supplier receives a request for access to Citrix Confidential Information or Information Systems and act upon Citrix's instruction concerning such request.

## Section 5: IT Security Standards

### 5.1 IT Security Controls

5.1.1 Supplier's Information Systems, Network Devices and Applications must be configured and deployed using a secure baseline (hardened) and unused ports/services must be disabled.

5.1.2 Supplier must implement controls to restrict connection times of idle/inactive sessions on Information Systems, Applications and Network Devices and terminate inactive sessions.

5.1.3 System clocks must be synchronized to a trusted time server source, maintaining accurate and synchronized time/time zone on all Information Systems and Network Devices and ensuring log files

have consistent time stamp information recorded.

5.1.4 Supplier must have defined security review processes for the deployment of new services that store/process Citrix Confidential Information.

5.1.5 Supplier must perform security assessments, scans and testing of Information Systems, Networks and Applications at planned intervals, at least annually, to verify compliance with organizational security policies and standards.

5.1.6 Supplier must maintain documented change management procedures that provide a consistent approach for controlling and identifying configuration changes for Information Systems, Applications and Network Devices.

### 5.2 Network Security

5.2.1 Supplier must implement and maintain network security infrastructure components such as firewalls, intrusion detection/prevention systems (IDS/IPS) and other security controls, providing detection, continuous monitoring, and restrictive network traffic flow to assist in limiting the impact of attacks.

5.2.2 Network traffic must be appropriately segregated, with routing and access controls separating traffic on internal Networks from public or other untrusted networks.

5.2.3 Remote access into the Supplier's Network must be approved and restricted to authorized Personnel only. Remote access must be controlled by secure access control protocols, encryption and two-factor authentication.

5.2.4 Supplier access to Citrix Networks and Information Systems must be via remote Virtual Desktop technology (VDI) only.

5.2.5 If VPN access (either site-to-site or IPsec) is used to access Citrix Networks and Information Systems, Supplier must segregate Computers that remotely connect to Citrix (using either physical segregation or VLAN subnets) to prevent Citrix Confidential Information, Networks and Information Systems from potentially being accessible or visible to unauthorized personnel. In no event may any Computer that has established a remote connection with Citrix Networks and Information Systems establish another connection to the Supplier or a separate client at the same time (known as split tunneling).

5.2.6 To the extent permitted by law, Citrix reserves the right to monitor Supplier access to and use of Citrix Information Systems, Networks and Applications ("Systems") for compliance with these Standards, and violations are subject to immediate removal of access.

### 5.3 Logging

5.3.1 Supplier must maintain logs from Information Systems, Network Devices and Applications for a minimum period of 90 days, unless otherwise stated in an Order. Logs must provide sufficient details to assist in the identification of the source of an issue and enable a sequence of events to be recreated.

5.3.2 Logs must record date, time and source location (IP address/hostname) for all access attempts. Logs must capture system and network security event information, alerts, failures, events and errors. Integrity of log files must be maintained and protected from tampering by restricting access to systems that store log information. Log files must be stored on a centralized log server.

### 5.4 Technical Vulnerability and Patch Management

5.4.1 Supplier must track information from vendors and other sources relating to technical vulnerabilities of operating systems, Applications, and Network Devices; and must promptly evaluate exposure to reported vulnerabilities to ensure that appropriate measures are taken to address potential risks.

5.4.2 Supplier must promptly apply patches for all operating systems, Applications and Network Devices according

to a documented vulnerability & patch management process and policy that requires patches be applied in a consistent, standardized manner and prioritized based on criticality and risk. If a security patch cannot be promptly applied due to requirements for testing, then effective risk mitigation controls must be implemented until such time that patches can be applied.

5.4.3 Where feasible, Computers must be configured to automatically receive operating system patches and updates from a centralized service that manages and distributes updates.

5.4.4 Supplier must use anti-virus/malware detection software to prevent, detect and remove malicious code. The software must provide automated signature updates. The software must detect if anti-virus/malware software on Computers has been disabled or not receiving regular updates.

5.4.5 Automatic virus and malware scanning checks must be carried out on all e-mail attachments sent to or received from external sources. Attachments identified as containing malicious code must be removed and deleted.

### 5.5 Account Management

5.5.1 Supplier must have user account management procedures to support the secure creation, amendment and deletion of accounts on Information Systems, Network Devices and Applications.

5.5.2 Supplier must ensure Information Systems, Applications and network device owners authorize all new user account requests and identify redundant accounts.

5.5.3 User accounts must have a unique login identifier and password. Supplier Personnel must not share account credentials.

### 5.6 Access Controls

5.6.1 Access controls must be implemented for Information Systems, Networks and Applications that verify the identity of all users and restrict access to authorized users. Access controls must use a role based access model based on the “least privilege” security principle and differentiate access levels for end-users and privileged access (e.g. systems administrators).

5.6.2 Access controls must be implemented for Information Systems, Networks and Applications that provide appropriate segregation of duties, e.g. different Personnel must perform the access authorization and access administration roles.

5.6.3 Access lists for Information Systems, Network Devices and Applications must be reviewed at least annually and access removed promptly when no longer required. Access to Citrix Information Systems, Networks and Applications by Supplier Personnel is limited to the purposes of performing Services as specified in the Agreement with Citrix.

### 5.7 Password Management

5.7.1 Strong password practices must be implemented, including minimum password length and complexity requirements (e.g., no dictionary words, use a mix of alpha numeric characters, require special characters, etc.).

5.7.2 Passwords may not be reused.

5.7.3 Passwords must have a defined expiration period not to exceed 90 days; alternatively, password practices may follow all requirements for memorized secrets found in National Institute of Standards and Technology (NIST) Special Publication 800-53B.

5.7.4 Passwords must be distributed separately from account information, in a manner that ensures confidentiality of information.

5.7.5 Passwords must be encrypted when transmitted between Information Systems, Network Devices and Applications and when stored.

### 5.8 Protection of Citrix Confidential Data

5.8.1 Supplier may access, use and process Citrix Confidential Information only on behalf of Citrix and only for the purposes specified in the Agreement with Citrix and in compliance with these Standards.

5.8.2 Citrix Confidential Information must be physically or logically separated (as applicable) from the confidential information of Supplier and its customers.

5.8.3 Supplier must delete or securely destroy Citrix Confidential Information upon Citrix's request, upon completion of Services or upon the termination of Services. Supplier may retain one copy of the foregoing materials, as required for regulatory retention purposes or by law, provided that any such copy is kept in encrypted format, is not used or accessed for any other purpose, and remains protected in accordance with the requirements of these Standards and is deleted promptly when no longer needed for such purpose.

5.8.4 Electronic Media containing Citrix Confidential Information must be sanitized before disposal using a process that assures complete data deletion and prevents data from being reconstructed or read, as prescribed in industry standards such as NIST SP 800-88 Revision 1 and DoD 5220.22-M. Defective Electronic Media containing Citrix Confidential Information must be physically destroyed.

5.8.5 Citrix Confidential Information must not be transmitted using unencrypted (plain text) channels or Services over public networks. Encrypted protocols protecting the transfer of information, for example, SFTP, TLS must be used (TLS version 1.2 or higher).

5.8.6 Secure e-mail transport using Transport Layer Security (TLS version 1.2 or higher) between Citrix mail gateways and Supplier mail gateways must be used to protect Citrix Confidential Information sent using e-mail.

### 5.9 Workstation, Device & Media Security

5.9.1 All Supplier resources providing Services to Citrix must use Supplier-provided laptop Computers only (not personal devices), except in cases where Citrix provides Supplier with laptop Computers to use. Such Supplier laptop Computers shall, at a minimum, include:

- A fully-encrypted hard drive (AES 128-bit or higher)
- A software agent that manages overall security compliance of the device and reports at least monthly to a central server
- A patching process that ensures Computers are current on all required security patches
- Blocks the installation of non-approved software
- Antivirus that conducts a scan at least a weekly
- Firewalls
- A data loss prevention tool
- Web filtering

Supplier shall handle Citrix-provided laptops using a reasonable duty of care designed to prevent loss, theft, damage and/or unauthorized access to the device (including not changing any security settings or programs installed) and otherwise in accordance with applicable controls specified herein.

5.9.2 Citrix Confidential Information may not be stored on external Electronic Media (e.g. USB memory storage, DVD, external drive), even if encrypted .

5.9.3 Citrix Confidential Information may not be stored on mobile devices unless encrypted using AES 128-bit or higher encryption and devices must be managed through centralized device management software, with the capability to remotely lock and wipe lost/stolen devices.

### 5.10 Computing Environments

5.10.1 Supplier will not permit the use of personal email accounts for exchanging, processing or storing Citrix Confidential Information.

5.10.2 Supplier will not use production systems that store or process Citrix Confidential Information for development, testing or staging purposes.

5.10.3 The use of public cloud storage Services for the storage/exchange of Citrix Confidential Information must be agreed and approved in writing by Citrix.

## Section 6: Back-up, Business Continuity and Disaster Recovery

### 6.1 Information Backup

6.1.1 Supplier must ensure Information Systems, Computers and software involved in the performance of the Services provided to Citrix are backed up to online and/or offline storage. Backups must be tested in accordance with operational backup standards.

6.1.2 Backup media leaving Supplier's facility must be protected against unauthorized access, misuse or corruption during transportation. Citrix Confidential Information stored on backup media must be encrypted using AES 256-bit or higher encryption.

6.1.3 If Supplier is storing Citrix Confidential Information on Citrix's behalf, Supplier must ensure daily backups, at a minimum.

### 6.2 Business Continuity and Disaster Recovery

6.2.1 Suppliers must have a Disaster Recovery (DR) program and maintain a documented organizational Business Continuity Plan (BCP). The DR program and BCP must be designed to prevent the loss of data and to ensure the Supplier can continue to function through operational interruption and continue to provide Services as specified in its Agreement with Citrix. Supplier will provide Citrix written summaries of its DR program and BCP upon request.

6.2.2 Supplier must ensure the scope of the BCP encompasses all locations, Personnel and Information Systems used to perform or provide Services for Citrix.

6.2.3 The BCP must be tested at least annually with documented results. The Supplier will provide confirmation of tests performed, including identified gaps and remediation actions or plans.

6.2.4 Supplier must promptly notify and report the potential impact to Citrix when the DR plan is executed.

## Section 7: Basic Physical and Environmental Security

### 7.1 Supplier Facilities

7.1.1 Supplier must maintain a physical security plan to protect offices and information processing Facilities that addresses internal and external threats to sites. Plans must be reviewed and updated on at least an annual basis.

7.1.2 Sites must have secure entry points that restrict access and protect against unauthorized access. Access to all

locations must be limited to authorized Personnel and approved visitors. All visitors must be logged and be escorted by Supplier Personnel at all times. Security guards, intrusion detection, and/or CCTV cameras must be used to monitor building entry points, loading and shipping docks, and public access areas. All visitors must be required to sign a visitor register.

7.1.3 Reception areas for offices and information processing Facilities must be manned by a receptionist or security guard. Out of hours access must be monitored, recorded and controlled. Logs detailing access must be stored for a period of at least 90 days.

7.1.4 Supplier Personnel and authorized visitors must be issued identification cards. Visitor identification cards must be distinguishable from Supplier Personnel identification.

7.1.5 Access cards and keys that provide access to secure areas and information processing Facilities such as data centers must be monitored and limited to authorized Personnel. Regular reviews of access rights to Facilities must be performed.

7.1.6 Off-site removal of Information Systems, servers and Network Devices must be restricted, approved and authorized appropriate security departments.

7.1.7 A clear desk policy must be enforced in areas where Citrix Confidential Information is stored. Documents that contain Citrix Confidential Information must be secured when not in use.

### 7.2 Citrix Facilities

7.2.1 Supplier Personnel are required to abide by Citrix's security requirements and direction when working at Citrix Facilities. The security measures employed at Citrix Facilities (e.g., use and placement of security cameras, use and placement of other physical and logical security controls) are Citrix Confidential Information. Personnel may not photograph or otherwise record Citrix Facilities or infrastructure, unless required for the performance of Services and Citrix approves in advance.

7.2.2 Supplier Personnel may not access Citrix Computers or Networks unless expressly authorized by Citrix Personnel.

## Section 8: Definitions

The following definitions apply to these Standards:

**"Agreement"** means an agreement between Citrix and a Supplier under which (a) Supplier performs Services for Citrix and (b) Supplier is provided access to Citrix Facilities, Network(s), Information Systems and/or Confidential Information.

**"Applications"** means middleware, databases, applications, web portals or other software that are used in the delivery of Services to Citrix.

**"Asset"** means any tangible Citrix owned item for which a Supplier has responsibility.

"**Computer**" means any desktop or laptop Computer, mobile device (e.g., cellular phone, Smartphone, tablet), server and/or storage device that (i) is involved in the performance of the Services, (ii) may be used to access a Network or an environment, or (iii) may access or store Confidential Information.

"**Information Systems**" means any system, including but not limited to development, test, stage and production systems, or storage/backup systems, that (a) are involved in the performance of the Services, (b) may access, process or store Citrix Confidential Information.

"**Confidential Information**" means all Citrix confidential information to which Supplier may be provided access in connection with the performance of Services, including without limitation Personal Information (PI); intellectual property (IP); source code; passwords; information concerning Citrix's customers, Suppliers or

partners; any data stored in or provided from the Information Systems of Citrix or its customers, Suppliers or partners; and any other Citrix Confidential Information as defined in an Agreement. References in this document to "Confidential Information" shall be deemed to include Confidential Information of Citrix customers, Suppliers or partners to which Supplier is provided access in connection with providing Services. Confidential Information shall also include any Citrix data that is subject to any data processing agreement between Citrix and Supplier, and any data subject to any data protection provisions in an Agreement.

**"Electronic Media"** means hard disk, solid state disk, DVD/CD, tape or any other form of media that can store electronic information.

**"Facilities"** means (a) any offices or data centers (whether owned or managed by Citrix, a Citrix customer, Supplier or a third-party) from which Citrix Confidential Information, Information Systems or Networks may be accessed. References in this document to (i) "Citrix Facilities" shall be deemed to include Facilities of Citrix customers, and (ii) "Supplier Facilities" shall be deemed to include third-party Facilities used by Supplier.

"**Network**" means any Citrix networks to which Supplier is provided access in connection with the performance of Services under an Agreement and/or any Supplier networks that are used to access Confidential Information or Information Systems.

"**Network devices**" means routers, switches, load balancers, firewalls and virtual private network (VPN) devices.

**"Partner"** means any organization that participates in any of the Citrix relationships described in https://www.citrix.com/partner-programs/ and, in connection with its participation in such relationship, (a) accesses Citrix or Citrix customer Facilities, Networks and/or Information Systems, or (b) accesses, processes, or stores Citrix Confidential Information.

**"Personnel"** means all Supplier employees, contractors, sub-contractors and agents who are provided access to Facilities, Networks, Information Systems and/or Confidential Information.

"**PI**" or "**Personal Information**" means any information to which Supplier is provided access that could identify any individual, either directly or indirectly, including without limitation the individual's name; address; government identification/national identification number; health, financial or employment information, phone number, e-mail address, IP address.

**"Product"** means a hardware or software component or assembled good manufactured for or supplied to Citrix.

**"Security Incident"** means (a) unauthorized access to Confidential Information or Information Systems, or (b) the loss of confidentiality integrity or availability of any Confidential Information,

"**Services**" means the work to be performed by Supplier for Citrix as specified in an Agreement, contract, or statement of work.

"**Vendor**" means an entity (including its Personnel) that performs Services under an Agreement,
"**Supplier Facilities**" means all Facilities used by Supplier, including third-party Facilities.

*Effective Date:* June 4, 2021