

# CERTIFICATE OF REGISTRATION

## Information Security Management System – ISO/IEC 27001:2013

Coalfire Certification, Inc. certifies that the following organization operates an Information Security Management System (ISMS) that conforms to the requirements of ISO/IEC 27001:2013 per the scope and boundaries statement detailed below:

<b>COMPANY:</b>	Citrix Systems, Inc.	<b>ADDRESS:</b>	851 West Cypress Creek Road Fort Lauderdale, FL 33309 United States
-----------------	----------------------	-----------------	---

### Scope:

The certificate scope comprises the Information Management System (IMS) supporting the operation underlying the following products and service offerings:

#### Citrix Cloud-Based Services:

- Citrix Cloud Platform & Identity Service
- Citrix DaaS (Desktop as a Service)
- Citrix Content Collaboration/SF (formerly known as ShareFile)
- Citrix Analytics Service

These activities are governed by the Statement of Applicability based on ISO/IEC 27001:2013 as extended by the Processor controls described within ISO/IEC 27701:2019. The organizational scope includes Compliance Risk Management, Information Security, Information Technology / Enterprise Operations, Product Engineering, Human Resources, Legal (Privacy & Compliance) and Global Security Risk Services.

### STATEMENT OF APPLICABILITY:

**VERSION:** 2022.7

ON BEHALF OF COALFIRE CERTIFICATION, INC.

**DATE:** July 7, 2022

### Original Registration Date:

December 3, 2019

### Certificate Issuance Date:

October 21, 2022

### Expiration Date:

December 3, 2025



David Forman, Director of Coalfire Certification, Inc.



This certificate relates to the Information Security Management System, and not to the products or services of the certified organization. The certification reference number, the mark of the certification body and/or the accreditation mark may not be shown on products or stated in documents regarding products or services. Promotional material, advertisements or other documents showing or referring to this certificate, the trademark of the certification body, or the accreditation mark, must comply with the intention of the certificate.

**Address:**

**Key Processes and Activities:**

<p>Central Office 851 West Cypress Creek Road Fort Lauderdale, FL 33309 United States</p>	<ul style="list-style-type: none"> <li>• Operational control and authority for the management system</li> <li>• Policy and procedure reviews</li> <li>• Cloud engineering services</li> <li>• System development</li> <li>• Application security</li> <li>• Background checks</li> <li>• Analysis of statutory and regulatory requirements</li> <li>• Facilities and property management</li> </ul>
<p>Satellite Office #2 101 Cambridge Science Park Road Milton, Cambridge Science Park Road Cambridge CB4 0FY United Kingdom</p>	<ul style="list-style-type: none"> <li>• Cloud engineering services</li> <li>• System development</li> <li>• Site reliability engineering</li> <li>• Background checks</li> <li>• Desktop engineering</li> <li>• Product management</li> <li>• Customer success and support</li> <li>• Facilities and property management</li> </ul>
<p>Data Center #1 50 NE 9<sup>th</sup> Street Miami, FL 33132 United States</p>	<ul style="list-style-type: none"> <li>• Data center services</li> </ul>



## 2022 - ISO 27001 Statement of Applicability Summary

ISO 27001 Control Area (Enterprise Level)	Number of ISO 27001 Controls	Number of Applicable ISO 27001 Controls (Enterprise Level)	% Controls applicable (Enterprise Level)	Number of Applicable Controls Implemented (Enterprise Level)	% Applicable Controls Implemented (Enterprise Level)
A.5 Information security policies	2	2	100%	2	100%
A.6 Organization of information security	7	7	100%	7	100%
A.7 Human resources security	6	6	100%	6	100%
A.8 Asset management	10	10	100%	10	100%
A.9 Access control	14	14	100%	14	100%
A.10 Cryptography	2	2	100%	2	100%
A.11 Physical and environmental security	15	15	100%	15	100%
A.12 Operations security	14	14	100%	14	100%
A.13 Communications security	7	7	100%	7	100%
A.14 System acquisition, development and maintenance	13	13	100%	13	100%
A.15 Supplier relationships	5	5	100%	5	100%
A.16 Information security incident management	7	7	100%	7	100%
A.17 Information security aspects of business continuity management	4	4	100%	4	100%
A.18 Compliance	8	8	100%	8	100%
<b>Total</b>	<b>114</b>	<b>114</b>		<b>114</b>	

ISO 27001 Control Area (Product Level Level)	Number of ISO 27001 Controls	Number of Applicable ISO 27001 Controls (Product Level)	% Controls applicable (Product Level)	Number of Applicable Controls Implemented (Product Level)	% Applicable Controls Implemented (Product Level)
A.5 Information security policies	2	2	100%	2	100%
A.6 Organization of information security	7	7	100%	7	100%
A.7 Human resources security	6	6	100%	6	100%
A.8 Asset management	10	10	100%	10	100%
A.9 Access control	14	14	100%	14	100%
A.10 Cryptography	2	2	100%	2	100%
A.11 Physical and environmental security	15	15	100%	15	100%
A.12 Operations security	14	14	100%	14	100%
A.13 Communications security	7	7	100%	7	100%
A.14 System acquisition, development and maintenance	13	13	100%	13	100%
A.15 Supplier relationships	5	5	100%	5	100%
A.16 Information security incident management	7	7	100%	7	100%
A.17 Information security aspects of business continuity management	4	4	100%	4	100%
A.18 Compliance	8	8	100%	8	100%
<b>Total</b>	<b>114</b>	<b>114</b>		<b>114</b>	