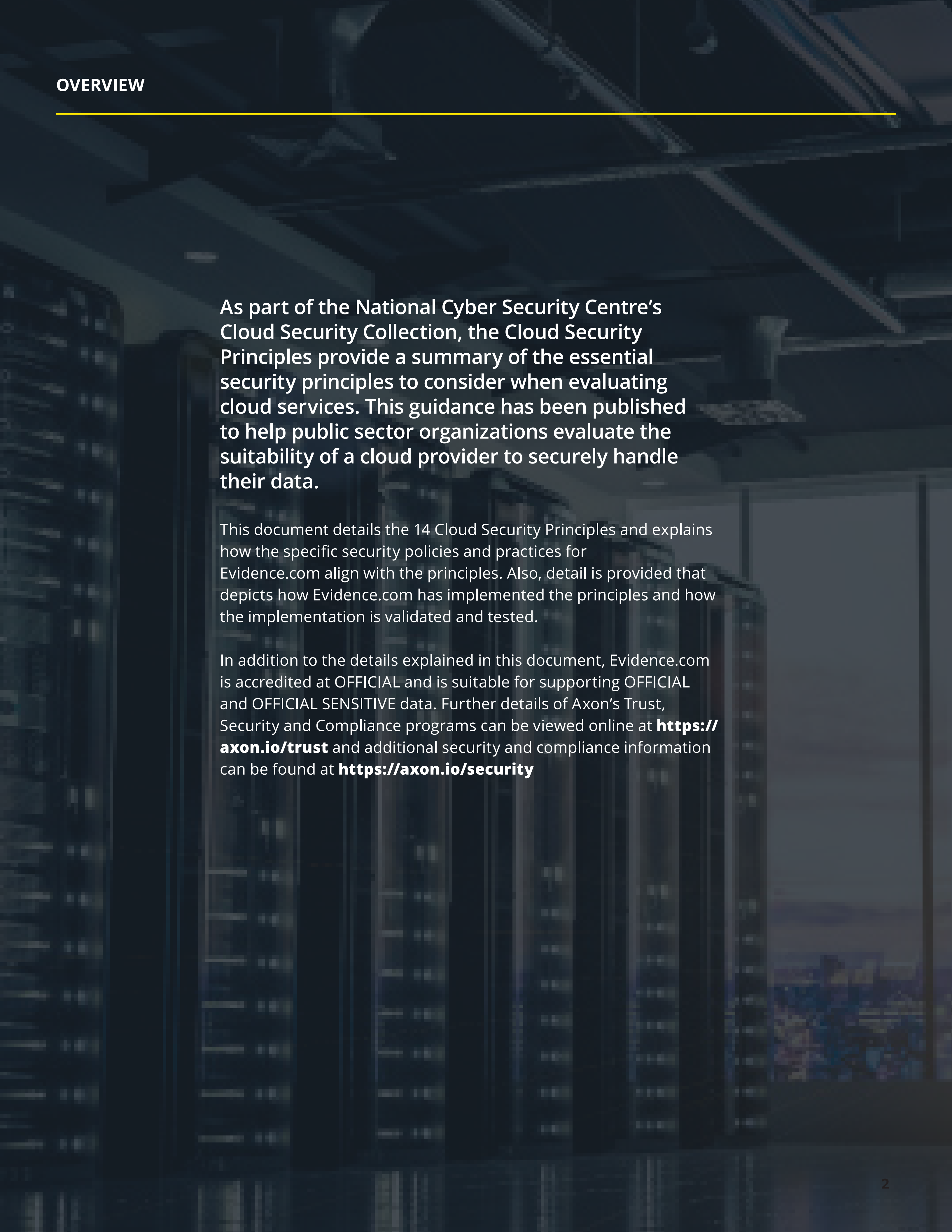
CLOUD SECURITY PRINCIPLES: EVIDENCE.COM IMPLEMENTATION DETAILS

PROTECT LIFE.
PROTECT TRUTH.



OVERVIEW

As part of the National Cyber Security Centre's Cloud Security Collection, the Cloud Security Principles provide a summary of the essential security principles to consider when evaluating cloud services. This guidance has been published to help public sector organizations evaluate the suitability of a cloud provider to securely handle their data.

This document details the 14 Cloud Security Principles and explains how the specific security policies and practices for Evidence.com align with the principles. Also, detail is provided that depicts how Evidence.com has implemented the principles and how the implementation is validated and tested.

In addition to the details explained in this document, Evidence.com is accredited at OFFICIAL and is suitable for supporting OFFICIAL and OFFICIAL SENSITIVE data. Further details of Axon's Trust, Security and Compliance programs can be viewed online at **https://axon.io/trust** and additional security and compliance information can be found at **https://axon.io/security**

#	Cloud Security Principle	Axon Compliance	Implementation Approach				Implementation Validation & Testing Programs		
			Service provider assertion	Contractual commitment	Independent validation of assertions	Independent testing of implementation	IT Health Check (ITHC)	ISO/IEC 27001:2013 Certification	CSA STAR Level 2 Attestation (SSAE-16 SOC 2+)
1	Data in transit protection	Axon maintains controls to protect and monitor boundaries of Evidence.com. These include firewalls, network segmentation, proxies, and intrusion detection systems. Evidence data transiting networks is encrypted with TLS 1.2 using 128 bits or stronger keys. FIPS 140-2 approved encryption ciphers (or stronger) are used, including AES 256, and RSA 2048. Additionally, Perfect Forward Secrecy is enabled. Axon maintains policies and practices for Evidence.com for encryption key and certificate management.		X		X	X	X	X
2	Asset protection and resilience	Evidence.com data centres are located within the UK. Customer data is not stored outside of the UK. Axon commits in contract that data will not be stored outside the UK. Axon Evidence.com data centres provide world-class physical protections and are ISO 27001 certified. When hard disks are taken out of service they are demagnetised and destroyed on site by our IaaS partner. Additionally, Axon Evidence.com stores evidence data in two geographically dispersed data centers to provide high levels of availability. This availability is backed by the Evidence.com Service Level Agreement.							
2.1	Physical location and legal jurisdiction			X					X
2.2	Data centre security			X	X			X	X
2.3	Data at rest protection				X		X		X
2.4	Data sanitisation				X			X	
2.5	Equipment disposal				X			X	
2.6	Physical resilience and availability			X	X				X

#	Cloud Security Principle	Axon Compliance	Implementation Approach				Implementation Validation & Testing Programs		
			Service provider assertion	Contractual commitment	Independent validation of assertions	Independent testing of implementation	IT Health Check (ITHC)	ISO/IEC 27001:2013 Certification	CSA STAR Level 2 Attestation (SSAE-16 SOC 2+)
3	Separation between consumers	Axon Evidence.com customers are logically separated at the application layer. The application and underlying infrastructure undergo at least five penetration tests a year that include in scope the separation between consumers. One of the five penetration test is an IT Health Check (ITHC) performed by a CESG approved CHECK security team.				X	X		X
4	Governance framework	Axon Evidence.com is ISO 27001 certified by a United Kingdom Accreditation Service (UKAS) recognized audit body. The Vice President of Information Security coordinates the information security governance program.			X			X	X
5	Operational security	Configuration and change management, vulnerability management, protective monitoring, and incident management are demonstrated by Axon Evidence.com's compliance with the ISO 27001 information security standard. Additional detail can be reviewed in Axon's Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) response: https://cloudsecurityalliance.org/star-registrant/axon/							
5.1	Configuration and change management				X		X	X	X
5.2	Vulnerability management				X	X	X	X	X
5.3	Protective monitoring				X			X	X
5.4	Incident management				X			X	X

#	Cloud Security Principle	Axon Compliance	Implementation Approach				Implementation Validation & Testing Programs		
			Service provider assertion	Contractual commitment	Independent validation of assertions	Independent testing of implementation	IT Health Check (ITHC)	ISO/IEC 27001:2013 Certification	CSA STAR Level 2 Attestation (SSAE-16 SOC 2+)
6	Personnel security	Axon personnel do not have access to a customer's evidence data without the explicit authorization from the customer. The only exception to this is for a small team of administrators who would only access evidence data in the event of a system emergency. All Axon personnel that may encounter customer evidence data as part of their job responsibilities are subject to the appropriate local adjudication processes. Many personnel have completed the UK BPSS or are SC cleared. Contractors are subject to the same personnel security screening and security education as Axon personnel. Axon conducts security education training on at least an annual basis.	X		X	X		X	X
7	Secure development	Axon includes security as part of the product development process and ongoing application maintainance. This is demonstrated by the ISO 27001 certification and is technically validated during the periodic penetration tests against Axon Evidence.com. Additional detail can be reviewed in Axon's Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) response: https://cloudsecurityalliance.org/star-registrant/axon/			X			X	X
8	Supply chain security	Axon leverages Infrastructure as a Service providers to deliver the Evidence.com service. Service providers must be at least ISO 27001 certified. Axon periodically reviews the security practices of the infrastructure providers to ensure Axon's security expectations are met.			X			X	
9	Secure consumer management	Within Axon Evidence.com, a force maintains full control over the administration and provisioning of user accounts within the service. Role-based access control can be utilized to define roles and permissions to evidence data and features of the service.							
9.1	Authentication of consumers to management interfaces and within support channels				X				X
9.2	Separation and access control within management interfaces				X		X		X

#	Cloud Security Principle	Axon Compliance	Implementation Approach				Implementation Validation & Testing Programs		
			Service provider assertion	Contractual commitment	Independent validation of assertions	Independent testing of implementation	IT Health Check (ITHC)	ISO/IEC 27001:2013 Certification	CSA STAR Level 2 Attestation (SSAE-16 SOC 2+)
10	Identity and authentication	Axon Evidence.com allows for forces to securely manage their usage of the service commensurate with their security risk profile. See https://www.axon.io/security for details.	X		X	X			X
11	External interface protection	The Axon Evidence.com application and underlying infrastructure undergo at least five penetration tests a year. One of the five penetration test is an IT Health Check (ITHC) performed by a CESG approved CHECK security team.			X	X	X		X
12	Secure service administration	Axon administers the Axon Evidence.com service through secure interfaces that require at least 2 factors for authentication. The administrative interfaces are included in scope for the ISO 27001 certification. End-user devices used to manage the service are managed and controlled by Axon and configured with a hardened OS, an anti-malware solution and full disk encryption.			X			X	X
13	Audit information provision to consumers	Axon Evidence.com maintains and provides to forces tamper-proof evidence audit records that log the when, who, and what for each evidence file. These records cannot be edited or changed, even by account administrators. User activity logging is available within the service to monitor users actions and authentication activity. Additionally, the service includes evidence deletion protection to monitor and recover evidence that may have been accidently deleted. These deletion protection features include deletion approval workflows, deletions notification emails, and a deletion remorse period.			X	X			X
14	Secure use of the service by the consumer	Axon Evidence.com provides detail of the security implications when using the service within the Evidence.com Service RMADS. Axon Evidence.com has many guides available to customers to educate and assist in administrating the service in a safe and secure manner. Additionally, Axon has a professional services and customer support team that can provide onsite or remote assistance related to the Axon Evidence.com service.			X				X

TASER | AXON

▲, ▲ AXON, Axon, TASER, and ø are trademarks of TASER International, Inc., some of which are registered in the US and other countries. For more information, visit www.taser.com/legal. All rights reserved. © 2016 TASER International, Inc.