

# AWS Response to CACP Information and Communication Technology Sub-Committee

Offsite Data Storage and Processing Best Practices

*May 2017*



© 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved.

## Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

## Contents

<b>Introduction</b>	<b>4</b>
<b>CACP Requirements</b>	<b>5</b>
<b>Vendor Requirements</b>	<b>6</b>
<b>Information Security Requirements</b>	<b>18</b>
<b>Data Centre Security Requirements</b>	<b>27</b>
<b>Personnel Security Requirements</b>	<b>32</b>
<b>Access Control Requirements</b>	<b>34</b>
<b>Document Revisions</b>	<b>38</b>

## Introduction

This document provides information that Canadian police agencies can use to help determine how AWS services support their requirements, and how to integrate AWS into the existing control framework that supports their IT environment. For more information about compliance on AWS, see [AWS Risk and Compliance Overview](https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Overview.pdf) ([https://d0.awsstatic.com/whitepapers/compliance/AWS\\_Risk\\_and\\_Compliance\\_Overview.pdf](https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Overview.pdf)).

The tables listed in [CACP Requirements](#) below address the requirements listed in the *Canadian Association of Chiefs of Police (CACP) Information and Communication Technology Sub-Committee's Offsite Data Storage and Processing Best Practices*. Further supporting details on AWS's alignment with the CACP Sub-Committee's best practices can be requested subject to a non-disclosure agreement with AWS. Please contact your AWS account representative.

# CACP Requirements

The following tables describe how AWS aligns with the CACP information storage requirements.

***Protected A** and **Protected B** refer to security levels that the Canadian government has defined for sensitive government information and assets. Unauthorized access to **Protected A** information could lead to “Injury to an individual, organization or government.” Unauthorized access to **Protected B** information could lead to “Serious injury to an individual, organization or government.”*

Values in **Protected A** and **Protected B** are set to the following possible states:

- **M** – Mandatory
- **H** – Highly Desirable
- **D** – Desirable

## Vendor Requirements

Requirement	Protected A	Protected B	Reference	AWS Responsibility
<b>24x7 managed tier 1 and tier 2 support.</b>	M	M	CJIS	AWS provides a variety of options for 24x7 tier 1 and tier 2 support at the Business Support level or better. For more information, see <a href="https://aws.amazon.com/premiumsupport/compare-plans/">https://aws.amazon.com/premiumsupport/compare-plans/</a> .
<b>Uptime Guarantee of a minimum of 99.9%.</b>	H	H	CACP-ICT	Each AWS service provides details on availability SLAs. For instance, Amazon EC2 has an availability SLA of 99.95% ( <a href="https://aws.amazon.com/ec2/sla">https://aws.amazon.com/ec2/sla</a> ) and Amazon S3 has an availability SLA of 99.99% ( <a href="https://aws.amazon.com/s3/sla">https://aws.amazon.com/s3/sla</a> ).

<p><b>Documented and proven configuration management processes.</b></p>	<p>M</p>	<p>M</p>	<p>MITS</p>	<p>AWS maintains a documented and proven configuration management process that is performed during information system design, development, implementation, and operation.</p>
<p><b>Documented and proven change control processes that adhere to ITIL service management processes.</b></p>	<p>M</p>	<p>M</p>	<p>MITS/CACP- ICT</p>	<p>AWS maintains change control processes that support the scale and complexity of the business and have been independently assessed.</p>
<p><b>Documented and proven incident response processes, including:</b></p> <ul style="list-style-type: none"> <li>• <b>Incident Identification</b></li> <li>• <b>Incident Response</b></li> <li>• <b>Incident Reporting</b></li> <li>• <b>Incident Recovery</b></li> <li>• <b>Post-Incident Analysis</b></li> </ul>	<p>M</p>	<p>M</p>	<p>MITS</p>	<p>The AWS incident response program (detection, investigation and response to incidents) has been developed in alignment with ISO 27001 standards.</p>

<p><b>Provide a current SOC Level 2 Compliance Report (if financial data is used or stored).</b></p>	M	M	CACP-ICT	<p>AWS provides access to its SOC 1 Type 2 and SOC 2 Type 2: Security &amp; Availability reports, subject to a nondisclosure agreement, while the SOC 3: Security &amp; Availability report is publicly available. For more information, see <a href="https://aws.amazon.com/compliance/soc-faqs/">https://aws.amazon.com/compliance/soc-faqs/</a>.</p>
<p><b>Maintain current PCI compliance (if PCI data is used or stored).</b></p>	M	M	CACP-ICT	<p>AWS maintains compliance with PCI-DSS v3.2 as a Level 1 service provider. For more information, see <a href="https://aws.amazon.com/compliance/pci-dss-level-1-faqs/">https://aws.amazon.com/compliance/pci-dss-level-1-faqs/</a>.</p>
<p><b>Maintain current Cloud Controls Matrix (CCM) compliance report and provide to the agency upon request.</b></p>	H	H	CACP-ICT	<p>AWS is listed on the CSA's Star registrant's page located at <a href="https://cloudsecurityalliance.org/star-registrant/amazon-aws/">https://cloudsecurityalliance.org/star-registrant/amazon-aws/</a>.</p>

<p><b>The Contractor must possess adequate disaster recovery and business continuity processes from a manmade or natural disaster. The Contractor must provide their business continuity and disaster recovery plan to customer upon request. The plans must include but is not limited to:</b></p> <ul style="list-style-type: none"> <li>• <b>How long it would take to recover from a disruption.</b></li> <li>• <b>How long it will take to switch to a backup site.</b></li> <li>• <b>The level of service and functionality provided by the backup site; and within what time frame the provider will recover the primary data and service.</b></li> <li>• <b>A report on how and how often the customer data is backed up.</b></li> </ul>	M	M	RCMP	<p>Customer resiliency in the cloud is transformed with the use of cloud. Businesses are using AWS to enable faster disaster recovery of critical IT systems and we provide a whitepaper (<a href="https://aws.amazon.com/blogs/aws/new-whitepaper-use-aws-for-disaster-recovery/">https://aws.amazon.com/blogs/aws/new-whitepaper-use-aws-for-disaster-recovery/</a>) on using AWS for disaster recovery. Customer resiliency is then not tied to any underlying infrastructure impacts. AWS maintains internal operational continuity processes including N+2 physical redundancy from generators to third party service providers at every data centre globally.</p>
<p><b>Ability to determine where all agency information is at all times including online data and backups.</b></p>	D	M	CACP-ICT	<p>When using AWS, customers have full control of the movement of their data with the ability to choose the region in which their data is kept.</p>

<p><b>Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels).</b></p>	H	M	CJIS	<p>AWS has a limited number of access points to the information system to allow for a more comprehensive monitoring of inbound and outbound communications and network traffic. These customer access points are called API end-points, which allow customers to establish a secure communication session with their storage or compute instances within AWS. Customers have the ability to deploy various tools and mechanisms to monitor traffic and activity such as VPC configurations, EC2 Security Groups, the AWS Web Application Firewall (WAF), as well as secure, encrypted connections. For more information, see <a href="https://aws.amazon.com/security/">https://aws.amazon.com/security/</a>.</p>
<p><b>Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use 24x7.</b></p>	D	M	CJIS	<p>AWS customers benefit from AWS services and technologies built from the ground up to provide resilience in the face of DDoS attacks to include services designed with an automatic response to DDoS to help minimize time to mitigate and reduce impact.</p> <p>The customer has broad latitude to implement similar capabilities within their customer environment to monitor system events, detect attacks, and provide identification of unauthorized use 24x7 to include vulnerability scanning and penetration testing. For more information, see <a href="https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June_2015.pdf">https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June_2015.pdf</a>.</p>
<p><b>Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device shall “fail closed” vs. “fail open”).</b></p>	D	M	CJIS	<p>AWS users have the ability to configure their services to operate in a number of ways compliant with fail-secure requirements.</p>

<p><b>Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces.</b></p>	D	H	CACP-ICT	<p>AWS does not operate publicly accessible information system components, such as public web servers, from within the cloud infrastructure. All external interaction with the infrastructure is through a set of well known, structured API end points. Internet facing servers in the customer's account are entirely within their operational control. For more information, see <a href="https://aws.amazon.com/whitepapers/aws-security-best-practices/">https://aws.amazon.com/whitepapers/aws-security-best-practices/</a>.</p>
<p><b>Data in transit is encrypted.</b></p>	H	M	MITS	<p>AWS provides several means for supporting encrypting data in transit. Encrypted IPSec tunnels can be created between a customer's endpoint and their VPC. For more information, see <a href="https://aws.amazon.com/vpc">https://aws.amazon.com/vpc</a>.</p>
<p><b>Data at rest (local or backups) is encrypted.</b></p>	H	M	MITS	<p>AWS provides a variety of options for encryption of data at rest. For instance, with S3, customers can securely upload or download data to Amazon S3 via the SSL-encrypted endpoints using the HTTPS protocol. Amazon S3 can automatically encrypt customer data at rest and gives several choices for key management. Alternatively, customers can use a client encryption library such as the Amazon S3 Encryption Client to encrypt data before uploading to Amazon S3.</p> <p>If desired, Amazon S3 can encrypt customer data at rest with server-side encryption (SSE); Amazon S3 will automatically encrypt customer data on write and decrypt your data on retrieval. When Amazon S3 SSE encrypts data at rest, it uses Advanced Encryption Standard (AES) 256-bit symmetric keys.</p>

				<p>There are three ways to manage the encryption keys with server-side encryption with Amazon S3:</p> <ul style="list-style-type: none"> <li>• SSE with Amazon S3 Key Management (SSE-S3): Amazon S3 will encrypt data at rest and manage the encryption keys</li> <li>• SSE with Customer-Provided Keys (SSE-C): Amazon S3 will encrypt data at rest using the customer encryption keys customers provide</li> <li>• SSE with AWS KMS (SSE-KMS): Amazon S3 will encrypt data at rest using keys only the customer manages in the AWS Key Management Service (KMS).</li> </ul> <p>For more information, see:</p> <ul style="list-style-type: none"> <li>• <a href="https://aws.amazon.com/s3/details/#security">https://aws.amazon.com/s3/details/#security</a></li> <li>• <a href="https://aws.amazon.com/kms/">https://aws.amazon.com/kms/</a></li> </ul>
<p><b>When encryption is employed, the cryptographic keys meet or exceed AES 256.</b></p>	<p>H</p>	<p>M</p>	<p>CACP-ICT</p>	<p>AWS supports the use of AES 256.</p>

<p><b>When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.</b></p>	D	H	MITS	<p>AWS GovCloud (US) provides endpoints compliance with FIPS 140-2 requirements. Customers have the ability to deploy FIPS compliant modules within their account depending on their application's ability to support FIPS 140-2 cryptographic modules.</p>
<p><b>Encryption keys be highly secured, protected and available to the agency upon request.</b></p>	M	M	MITS	<p>The use of AWS CloudHSM or AWS KMS provides the options for customers to create and control their own encryption keys.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> <li>• <a href="https://aws.amazon.com/kms/">https://aws.amazon.com/kms/</a></li> <li>• <a href="https://aws.amazon.com/cloudhsm/">https://aws.amazon.com/cloudhsm/</a></li> </ul>
<p><b>Encryption keys are controlled and stored by the agency.</b></p>	D	H	CACP-ICT	<p>The use of AWS CloudHSM or AWS KMS provides the options for customers to create and control their own encryption keys.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> <li>• <a href="https://aws.amazon.com/kms/">https://aws.amazon.com/kms/</a></li> <li>• <a href="https://aws.amazon.com/cloudhsm/">https://aws.amazon.com/cloudhsm/</a></li> </ul>

<p><b>External access to the administrative or management functions must be over VPN only. This includes modems, FTP, or any protocol/port support provided by the equipment manufacturer. This access must be limited to users with two-factor authentication.</b></p>	<p>D</p>	<p>H</p>	<p>NPISAB</p>	<p>Customers can connect to the management console to administer their environment over VPN and mandate the use of two-factor authentication per internal agency requirements. For more information, see <a href="https://aws.amazon.com/iam/details/mfa/">https://aws.amazon.com/iam/details/mfa/</a>. AWS infrastructure administrative connections to the AWS infrastructure are performed using secure mechanisms.</p>
<p><b>Agency data shall not be used by any service provider for any purposes. The service provider shall be prohibited from scanning data files for the purpose of data mining or advertising.</b></p>	<p>M</p>	<p>M</p>	<p>CACP-ICT</p>	<p>AWS does not access or use customer content for any purpose other than as legally required and for maintaining the AWS services and providing them to customers and their end users. AWS never uses customer content or derives information from it for marketing or advertising. For more information, see <a href="https://aws.amazon.com/compliance/data-privacy-faq/">https://aws.amazon.com/compliance/data-privacy-faq/</a>.</p> <p>The AWS Privacy Policy describes how AWS collects and uses information that customers provide in connection with the creation or administration of AWS accounts, which is referred to as "Account Information." For example, Account Information includes names, usernames, phone numbers, email addresses and billing information associated with a customer's AWS account.</p> <p>The AWS Privacy Policy applies to customers' Account Information and does not apply to the content that customers store on AWS, including any personal information of customer end users. AWS will not disclose, move, access or use customer content except as provided in the customer's agreement with AWS. The customer agreement with AWS (<a href="https://aws.amazon.com/agreement/">https://aws.amazon.com/agreement/</a>) and the AWS Data Protection FAQ contain more information about how we handle content you store on our systems.</p>

<p><b>All firewalls meet the minimum standard of Evaluation Assurance Level (EAL) 4.</b></p>	H	M	NPISAB	<p>AWS provides multiple features and services to help customers protect data including the AWS Web Application Firewall (WAF). There are also several vendors in the AWS Marketplace with similar security utility product offerings.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> <li>• <a href="https://aws.amazon.com/waf/">https://aws.amazon.com/waf/</a></li> <li>• <a href="https://aws.amazon.com/marketplace">https://aws.amazon.com/marketplace</a></li> </ul>
<p><b>Ensure regular virus, malware &amp; penetration testing of their environment.</b></p>	M	M	NPISAB	<p>AWS ensures regular virus, malware, and penetration testing of the infrastructure environment. Customers can also conduct their own penetration testing within their account. For more information, see <a href="https://aws.amazon.com/security/penetration-testing/">https://aws.amazon.com/security/penetration-testing/</a>.</p>
<p><b>Provide sufficient documentation of their virus, malware &amp; penetration testing results, and upon request by the agency, the vendor will provide a current report.</b></p>	H	M	CACP-ICT	<p>AWS' program, processes and procedures for managing antivirus/malicious software are in alignment with the ISO 27001 standard and are referenced in AWS SOC reports. AWS Security regularly engages independent security firms to perform external vulnerability threat assessments and has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.</p>

<p><b>Provide sufficient documentation of all patch management and upon request by the agency, the vendor will provide a current report.</b></p>	H	M	CACP-ICT	<p>Customers retain control of their own guest operating systems, software, and applications, and are responsible for performing vulnerability scans and patching of their own systems. Customers can request permission to conduct scans of their cloud infrastructure as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy.</p> <p>AWS regularly scans all Internet-facing service endpoint IP addresses for vulnerabilities. AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. AWS' own maintenance and system patching generally do not impact customers.</p> <p>For more information see AWS Security Whitepaper (available at <a href="https://aws.amazon.com/security/">https://aws.amazon.com/security/</a>) and ISO 27001 standard, Annex A, domain 12.</p> <p>AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.</p>
<p><b>Continual monitoring and logging for the following events:</b></p> <ul style="list-style-type: none"> <li>• <b>DDOS attacks</b></li> <li>• <b>Unauthorized changes to the system hardware, firmware and software</b></li> <li>• <b>System performance anomalies</b></li> <li>• <b>Known attack signatures</b></li> </ul>	D	M	MITS	<p>AWS employs a variety of tools and techniques to monitor network events and unauthorized use 24x7. AWS customers benefit from AWS services and technologies built from the ground up to provide resilience in the face of DDoS attacks including services designed with an automatic response to DDoS to help minimize time to mitigate and reduce impact.</p> <p>The customer has broad latitude to implement similar capabilities within their customer environment to monitor system events, detect attacks, and provide identification of unauthorized use 24x7.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> <li>• <a href="https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf">https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf</a></li> <li>• <a href="https://aws.amazon.com/security">https://aws.amazon.com/security</a></li> </ul>

<b>Ability to enable data retention policies as defined by the customer.</b>	D	H	CACP-ICT	<p>While AWS provides customers with the ability to delete their data, AWS customers retain control and ownership of their data and are responsible for managing data retention to their own requirements.</p> <p>AWS maintains data retention policies in accordance with several well-known international standards and regulations such as SOC and PCI-DSS that are independently assessed and attested.</p>
--	---	---	----------	---

## Information Security Requirements

Requirement	Protected A	Protected B	Reference	AWS Responsibility
<b>Ability to determine where all agency information is at all times including online data and backups.</b>	D	M	CACP-ICT	Customers have full control of the movement of their data when using AWS with the choice of the region in which their data is kept.
<b>Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels).</b>	H	M	CJIS	AWS has a limited number of access points to the information system to allow for a more comprehensive monitoring of inbound and outbound communications and network traffic. These customer access points are called API end-points, which allow customers to establish a secure communication session with their storage or compute instances within AWS. Customers have the ability to deploy various tools and mechanisms to monitor traffic and activity such as VPC configurations, EC2 Security Groups, the AWS Web Application Firewall (WAF), as well as secure, encrypted connections. For more information, see <a href="https://aws.amazon.com/security/">https://aws.amazon.com/security/</a> .

<p><b>Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use 24x7.</b></p>	<p>D</p>	<p>M</p>	<p>CJIS</p>	<p>AWS customers benefit from AWS services and technologies built from the ground up to provide resilience in the face of DDoS attacks to include services designed with an automatic response to DDoS to help minimize time to mitigate and reduce impact.</p> <p>The customer has broad latitude to implement similar capabilities within their customer environment to monitor system events, detect attacks, and provide identification of unauthorized use 24x7 to include vulnerability scanning and penetration testing. For more information, see</p> <ul style="list-style-type: none"> <li>• <a href="https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf">https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf</a></li> <li>• <a href="https://aws.amazon.com/security">https://aws.amazon.com/security</a></li> <li>• <a href="https://aws.amazon.com/security/penetration-testing/">https://aws.amazon.com/security/penetration-testing/</a></li> </ul>
<p><b>Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device shall “fail closed” vs. “fail open”).</b></p>	<p>D</p>	<p>M</p>	<p>CJIS</p>	<p>Users in AWS have the ability to configure their services to operate in a number of ways compliant with fail-secure requirements.</p>

<p><b>Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces.</b></p>	D	H	CACP-ICT	<p>AWS does not operate publicly accessible information system components such as public web servers from within the cloud infrastructure. All external interaction with the infrastructure is through a set of well known, structured API end points. Internet facing servers in the customer's account are entirely within their operational control.</p> <p>For more information, see <a href="https://aws.amazon.com/whitepapers/aws-security-best-practices/">https://aws.amazon.com/whitepapers/aws-security-best-practices/</a>.</p>
<p><b>Data in transit is encrypted.</b></p>	H	M	MITS	<p>AWS provides several options for supporting encrypting data in transit. Encrypted IPsec tunnels can be created between a customer's endpoint and their VPC. For more information, see <a href="https://aws.amazon.com/vpc">https://aws.amazon.com/vpc</a>.</p>
<p><b>Data at rest (local or backups) is encrypted.</b></p>	H	M	MITS	<p>AWS provides a variety of options for encryption of data at rest. For example, with S3, customers can securely upload or download data to Amazon S3 via the SSL-encrypted endpoints using the HTTPS protocol. Amazon S3 can automatically encrypt customer data at rest and offers several choices for key management. Alternatively, customers can use a client encryption library such as the Amazon S3 Encryption Client to encrypt data before uploading to Amazon S3.</p> <p>If desired, Amazon S3 can encrypt customer data at rest with server-side encryption (SSE); Amazon S3 will automatically encrypt customer data on write and decrypt your data on retrieval. When Amazon S3 SSE encrypts data at rest, it uses Advanced Encryption Standard (AES) 256-bit symmetric keys. There are three ways to</p>

				<p>manage the encryption keys with server-side encryption with Amazon S3:</p> <ul style="list-style-type: none"> <li>• SSE with Amazon S3 Key Management (SSE-S3): Amazon S3 will encrypt data at rest and manage the encryption keys;</li> <li>• SSE with Customer-Provided Keys (SSE-C): Amazon S3 will encrypt data at rest using the customer encryption keys customers provide; or,</li> <li>• SSE with AWS KMS (SSE-KMS): Amazon S3 will encrypt data at rest using keys only the customer manages in the AWS Key Management Service (KMS).</li> </ul> <p>For more information, see</p> <ul style="list-style-type: none"> <li>• <a href="https://aws.amazon.com/s3/details/#security">https://aws.amazon.com/s3/details/#security</a></li> <li>• <a href="https://aws.amazon.com/kms">https://aws.amazon.com/kms</a></li> </ul>
<p><b>When encryption is employed, the cryptographic keys meet or exceed AES 256.</b></p>	<p>H</p>	<p>M</p>	<p>CACP-ICT</p>	<p>AWS supports the use of AES 256.</p>

<p><b>When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.</b></p>	D	H	MITS	<p>AWS GovCloud (US) provides endpoints compliance with FIPS 140-2 requirements. Customers have the ability to deploy FIPS compliant modules within their account depending on their application's ability to support FIPS 140-2 cryptographic modules.</p> <p>For more information, see <a href="https://aws.amazon.com/federal/">https://aws.amazon.com/federal/</a>.</p>
<p><b>Encryption keys be highly secured, protected and available to the agency upon request.</b></p>	M	M	MITS	<p>The use of AWS CloudHSM or AWS KMS provides the options for customers to create and control their own encryption keys.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> <li>• <a href="https://aws.amazon.com/kms/">https://aws.amazon.com/kms/</a></li> <li>• <a href="https://aws.amazon.com/cloudhsm/">https://aws.amazon.com/cloudhsm/</a></li> </ul>
<p><b>Encryption keys are controlled and stored by the agency.</b></p>	D	H	CACP-ICT	<p>The use of AWS CloudHSM or AWS KMS provides the options for customers to create and control their own encryption keys.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> <li>• <a href="https://aws.amazon.com/kms/">https://aws.amazon.com/kms/</a></li> <li>• <a href="https://aws.amazon.com/cloudhsm/">https://aws.amazon.com/cloudhsm/</a></li> </ul>

<p><b>External access to the administrative or management functions must be over vpn only. This includes modems, ftp, or any protocol/port support provided by the equipment manufacturer. This access must be limited to users with two-factor authentication.</b></p>	<p>D</p>	<p>H</p>	<p>NPISAB</p>	<p>Customers can connect to the management console to administer their environment over VPN and mandate the use of two-factor authentication per internal agency requirements. For more information, see <a href="https://aws.amazon.com/iam/details/mfa/">https://aws.amazon.com/iam/details/mfa/</a>. AWS infrastructure administrative connections to the AWS infrastructure are performed using secure mechanisms.</p>
<p><b>Agency data shall not be used by any service provider for any purposes. The service provider shall be prohibited from scanning data files for the purpose of data mining or advertising.</b></p>	<p>M</p>	<p>M</p>	<p>CACP-ICT</p>	<p>AWS does not access or use customer content for any purpose other than as legally required and for maintaining the AWS services and providing them to customers and their end users. AWS never uses customer content or derives information from it for marketing or advertising. For more information, see <a href="https://aws.amazon.com/compliance/data-privacy-faq/">https://aws.amazon.com/compliance/data-privacy-faq/</a>. The AWS Privacy Policy describes how AWS collects and uses information that customers provide in connection with the creation or administration of AWS accounts, which is referred to as “Account Information.” For example, Account Information includes names, usernames, phone numbers, email addresses and billing information associated with a customer’s AWS account. The AWS Privacy Policy applies to customers’ Account Information and does not apply to the content that customers store on AWS, including any personal information of customer end users. AWS will not disclose, move, access or use customer content except as provided in the customer’s agreement with AWS. The customer agreement with AWS (<a href="https://aws.amazon.com/agreement/">https://aws.amazon.com/agreement/</a>) and the AWS Data Protection FAQ contain more information about how we handle content you store on our systems.</p>

<p><b>All firewalls meet the minimum standard of Evaluation Assurance Level (EAL) 4.</b></p>	H	M	NPISAB	<p>AWS provides multiple features and services to help customers protect data including the AWS Web Application Firewall (WAF). There are also several vendors in the AWS Marketplace with similar security utility product offerings.</p> <p>For more information, see</p> <ul style="list-style-type: none"> <li>• <a href="https://aws.amazon.com/waf/">https://aws.amazon.com/waf/</a></li> <li>• <a href="https://aws.amazon.com/marketplace">https://aws.amazon.com/marketplace</a></li> </ul>
<p><b>Ensure regular virus, malware &amp; penetration testing of their environment.</b></p>	M	M	NPISAB	<p>AWS ensures regular virus, malware, and penetration testing of the infrastructure environment. Customers can also conduct their own penetration testing within their account.</p> <p>For more information, see <a href="https://aws.amazon.com/security/penetration-testing/">https://aws.amazon.com/security/penetration-testing/</a>.</p>
<p><b>Provide sufficient documentation of their virus, malware &amp; penetration testing results, and upon request by the agency, the vendor will provide a current report.</b></p>	H	M	CACP-ICT	<p>Customers retain control of their own guest operating systems, software, and applications, and are responsible for performing vulnerability scans and patching of their own systems. Customers can request permission to conduct scans of their cloud infrastructure as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy.</p> <p>AWS regularly scans all Internet-facing service endpoint IP addresses for vulnerabilities. AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. AWS' own maintenance and system patching generally do not impact customers.</p>

				<p>For more information see AWS Security Whitepaper (available at <a href="https://aws.amazon.com/security/">https://aws.amazon.com/security/</a>) and ISO 27001 standard, Annex A, domain 12.</p> <p>AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard</p>
<p><b>Provide sufficient documentation of all patch management and upon request by the agency, the vendor will provide a current report.</b></p>	<p>H</p>	<p>M</p>	<p>CACP-ICT</p>	<p>Customers retain control of their own guest operating systems, software, and applications, and are responsible for performing vulnerability scans and patching of their own systems. Customers can request permission to conduct scans of their cloud infrastructure as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy.</p> <p>AWS regularly scans all Internet-facing service endpoint IP addresses for vulnerabilities. AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. AWS' own maintenance and system patching generally do not impact customers.</p> <p>For more information see AWS Security Whitepaper (available at <a href="https://aws.amazon.com/security/">https://aws.amazon.com/security/</a>) and ISO 27001 standard, Annex A, domain 12.</p> <p>AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard</p>

<p><b>Continual monitoring and logging for the following events:</b></p> <ul style="list-style-type: none"> <li>• <b>DDOS Attacks</b></li> <li>• <b>Unauthorized changes to the system hardware, firmware and software</b></li> <li>• <b>System performance anomalies</b></li> <li>• <b>Known attack signatures</b></li> </ul>	D	M	MITS	<p>AWS employs a variety of tools and techniques to monitor network events and unauthorized use 24x7. AWS customers benefit from AWS services and technologies built from the ground up to provide resilience in the face of DDoS attacks including services designed with an automatic response to DDoS to help minimize time to mitigate and reduce impact.</p> <p>The customer has broad latitude to implement similar capabilities within their customer environment to monitor system events, detect attacks, and provide identification of unauthorized use 24x7.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> <li>• <a href="https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf">https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf</a></li> <li>• <a href="https://aws.amazon.com/security">https://aws.amazon.com/security</a></li> </ul>
<p><b>Ability to enable data retention policies as defined by the customer.</b></p>	D	H	CACP-ICT	<p>While AWS provides customers with the ability to delete their data, AWS customers retain control and ownership of their data and are responsible for managing data retention to their own requirements.</p> <p>AWS maintains data retention policies in accordance with several well-known international standards and regulations such as SOC and PCI-DSS that are independently assessed and attested.</p>

## Data Centre Security Requirements

Requirement	Protected A	Protected B	Reference	AWS Responsibility
<b>The data centre must be physically secured against the entry of unauthorized personnel.</b>	H	M	MIT5	<p>AWS strictly controls access to data centres, even for internal employees. Physical access to all AWS data centres housing IT infrastructure components is restricted to authorized data centre employees, vendors, and contractors who require access in order to execute their jobs. AWS data centres utilize trained security guards 24x7.</p> <p>Due to the fact that our data centres host multiple customers, AWS does not allow data center tours by customers, as this exposes a wide range of customers to physical access of a third party. To meet this customer need, an independent and competent auditor validates the presence and operation controls as part of our SOC 1, Type II report. This broadly accepted third-party validation provides customers with the independent perspective of the effectiveness of controls in place.</p>
<b>Locked doors, with access control systems that restrict entry to authorized parties only. All activity must be logged.</b>	H	M	RCMP	Physical access to the AWS data centres is controlled by an access control system and all activity is logged.

<b>Logs of personnel access privilege shall be kept for a minimum of one year, and provided to the agency upon request.</b>	D	M	CACP-ICT	Physical access logs are maintained for a minimum of one year. Access logs are provided to independent auditors in support of our formal compliance audits.
<b>Logs of personnel access changes shall be kept for a minimum of one year, and provided to the agency upon request.</b>	D	M	CJIS	Physical access logs are maintained for a minimum of one year.
<b>Building must be constructed with walls that are difficult to breach.</b>	D	M	RCMP	Buildings are constructed according to local building code (typically concrete).

<p><b>Two-factor authentication to enter the building containing the data centre.</b></p>	<p>D</p>	<p>H</p>	<p>MITS</p>	<p>Access to AWS data centres requires a variety of two-factor authentication mechanisms.</p>
<p><b>CCTV Video displayed and recorded for all entry and exit paths and building exterior.</b></p>	<p>D</p>	<p>M</p>	<p>CACP-ICT</p>	<p>CCTV systems are in use for every AWS data centre with recorded video.</p>
<p><b>24x 7 guard personnel at all main entry points to the building. Bags and packages will be examined upon entry.</b></p>	<p>D</p>	<p>M</p>	<p>CJIS</p>	<p>AWS uses guard personnel at all main entry points 24x7 with bag searches in place.</p>

<p><b>Authenticate visitors before authorizing escorted access to the data centre.</b></p>	<p>H</p>	<p>M</p>	<p>CJIS</p>	<p>Physical access to all AWS data centres housing IT infrastructure components is restricted to authorized data centre employees, vendors, and contractors who require access in order to execute their jobs and includes the escorting of visitors where applicable.</p>
<p><b>All customer information must be logically (and/or physically) separated from all other customer's information. This separation must be tested by an unbiased third party or demonstrated by the data centre management.</b></p>	<p>D</p>	<p>H</p>	<p>CJIS</p>	<p>All customer information is logically separated by default through the use of the Amazon Virtual Private Cloud (VPC) service – a service that has been assessed by multiple third party assessors. For more information, see <a href="https://aws.amazon.com/vpc/">https://aws.amazon.com/vpc/</a>.</p>
<p><b>Ability to indicate and limit which data centres agency data will be stored in.</b></p>	<p>D</p>	<p>M</p>	<p>CACP-ICT</p>	<p>The location of customer data is determined by the customer at the region level. AWS does not access, use, or move customer content for any purpose other than as legally required and for maintaining the AWS services and providing them to customers and their end users.</p>

<p><b>Agency information kept within a secure server room (SSR) that includes the following:</b></p> <ul style="list-style-type: none"> <li>• <b>Vibration detection on walls</b></li> <li>• <b>Intrusion detection system inside the secure server room</b></li> <li>• <b>Two person authentication to enter the secure server room</b></li> </ul>	D	H	RCMP	<p>AWS utilizes several layers of security to protect the server rooms within the data centre (“red zones”). AWS employs several physical security mechanisms including intrusion detection systems and two-person authentication.</p>
<p><b>Disposal of hard drives with agency information includes the following steps to meet Canadian Standard ITSG-06:</b></p> <ol style="list-style-type: none"> <li><b>1. Disk Encryption or overwriting</b></li> <li><b>2. Grind or hammer-mill into at least three pieces</b></li> </ol>	D	M	RCMP	<p>AWS uses multiple steps during the process of media decommissioning for both magnetic hard drives (HDD) and solid state drives (SSD). On site, HDDs are degaussed and then bent to an abrupt angle and SSDs are logically overwritten before being punched. Both types of drives are ultimately shredded for recycling of materials. Customers have the ability to conduct a variety of sanitization methods themselves including data deletion using relevant tools or encrypting data and destroying the encryption key rendering the data permanently unusable.</p>

## Personnel Security Requirements

Requirement	Protected A	Protected B	Reference	AWS Responsibility
<b>All system administrators and personnel with access to the facility must have Enhanced Security Check completed by a substantive law enforcement agency. A Canadian federal security clearance of level Secret or higher may be substituted and considered equivalent. A US federal security clearance of level Secret or higher may be substituted and considered equivalent.</b>	H	M	RCMP	All AWS employees must complete a comprehensive pre-employment background check. Several specific positions are also processed through a separate Trusted Position Check. Additionally, there are many employees that hold or are otherwise processed for a U.S. national security clearance (TS/SCI) (reinvestigated every five years) and/or Criminal Justice Information Services (CJIS) fingerprint and records check.
<b>Personnel must have initial background checks at the time of first employment with the Data Centre owner. Security clearances must be maintained within the expiry period. All system administrators and personnel with access to the facility must have the background check repeated on a five-year cycle.</b>	H	M	RCMP	All AWS employees must complete a comprehensive pre-employment background check. Several specific positions are also processed through a separate Trusted Position Check. Additionally, there are many employees that hold or are otherwise processed for a U.S. national security clearance (TS/SCI) (reinvestigated every five years) and/or Criminal Justice Information Services (CJIS) fingerprint and records check.  Employees with physical access are not provisioned logical access.

<p><b>Upon termination of individual employment, shall immediately terminate access to the facility.</b></p>	<p>M</p>	<p>M</p>	<p>RCMP</p>	<p>Upon termination, all employees' access to systems and facilities are revoked immediately.</p>
<p><b>Must maintain a list of personnel who have been authorized system or physical access to the data centre and its systems, and upon request provide a current copy to the agency.</b></p>	<p>H</p>	<p>M</p>	<p>CJIS</p>	<p>AWS maintains a list of employees with physical access as granted through the process to receive physical access. Logical access lists are retained as part of the LDAP permission group structure and does not constitute a consolidated list for distribution. All access management for both physical and logical are independently audited by multiple third party auditors for several formal compliance programs.</p>
<p><b>The Contractor must enforce separation of job duties, require commercially reasonable non-disclosure agreements and limit staff knowledge of customer data to that which is absolutely needed to perform to work.</b></p>	<p>H</p>	<p>M</p>	<p>RCMP</p>	<p>AWS rigorously employs the principles of least privilege, separation of roles and responsibilities, and disclosure of information on a need to know basis.</p>

## Access Control Requirements

Requirement	Protected A	Protected B	Reference	AWS Responsibility
<p><b>A password minimum length will be 8 characters and will have 3 of the 4 complexity requirements:</b></p> <ul style="list-style-type: none"> <li>• <b>Upper case</b></li> <li>• <b>Lower case</b></li> <li>• <b>Special characters</b></li> <li>• <b>Numeric Characters</b></li> </ul>	H	M	CJIS	<p>Access to the AWS infrastructure requires multi-factor authentication to include password complexity requirements.</p> <p>Customers can implement this requirement within their account, which AWS does not manage on their behalf.</p>
<p><b>The following password rules are implemented:</b></p> <ul style="list-style-type: none"> <li>• <b>A password re-use restriction will be used</b></li> <li>• <b>Password lifespans will be implemented and the time is configurable by the agency (standard 90 days)</b></li> <li>• <b>Not be a dictionary word or proper name</b></li> <li>• <b>Not be the same as the user ID</b></li> <li>• <b>Not be identical to the previous 6 passwords</b></li> <li>• <b>Must be transmitted and stored in an encrypted state</b></li> </ul>	H	M	CJIS/NPISAB	<p>Access to the AWS infrastructure requires multi-factor authentication to include password complexity and protection requirements.</p> <p>Customers can implement this requirement within their account, which AWS does not manage on their behalf.</p>

<ul style="list-style-type: none"> <li>• <b>Not be displayed when entered</b></li> <li>• <b>Automatic storage and caching of passwords by applications must be disabled</b></li> </ul>				
<p><b>User lockout after failed login attempts will be implemented and the count is configurable by the agency (default to 5).</b></p>	M	M	CJIS/NPISAB	Customers can implement this requirement within their account, which AWS does not manage on their behalf.
<p><b>Password reset will leverage automated email personal identity verification questions.</b></p>	M	M	CACP-ICT	Customers can implement this requirement within their account, which AWS does not manage on their behalf.

<p><b>Policy exist to ensure passwords must not be emailed or given over the phone.</b></p>	M	M	CACP-ICT	Customers can implement this requirement within their account, which AWS does not manage on their behalf.
<p><b>When using a Personal Identification Number (PIN) as a standard authenticator, the following rules are implemented:</b></p> <ul style="list-style-type: none"> <li>• <b>Must be a minimum of 6 digits</b></li> <li>• <b>Have no repeating digits (e.g. 112233)</b></li> <li>• <b>Have no sequential patterns (e.g. 12345)</b></li> <li>• <b>Expire within a maximum of 365 days (unless PIN is second factor)</b></li> <li>• <b>Not be identical to previous 3 PINS</b></li> <li>• <b>Must be transmitted and stored in an encrypted state</b></li> <li>• <b>Not be displayed when entered</b></li> </ul>	H	M	CJIS	Customers can implement this requirement within their account, which AWS does not manage on their behalf.

<p><b>System activity timer that will redirect user to the login page after a specific time that is configurable by the agency (Session Lock) (default to 30 mins).</b></p>	M	M	CJIS	Customers can implement this requirement within their account, which AWS does not manage on their behalf.
<p><b>The information system shall display an agency configurable system use message notification message.</b></p>	D	H	CJIS	Customers can implement this requirement within their account, which AWS does not manage on their behalf.
<p><b>Continual monitoring and logging for the following events:</b></p> <ul style="list-style-type: none"> <li>• <b>Successful and Unsuccessful login attempts</b></li> <li>• <b>Successful and Unsuccessful attempts to view/modify/delete permissions, files, directory or system resources</b></li> </ul>	D	M	MITS	AWS maintains logging and monitoring requirements in accordance with a variety of standards and requirements to include ISO 27001, SOC, PCI DSS, FedRAMP, U.S. Department of Defense Cloud Computing Security Requirements Guidance (DoD CC SRG), CJIS, and others covering these requirements.

<ul style="list-style-type: none"> <li>• <b>Successful and Unsuccessful attempts to change account passwords</b></li> <li>• <b>Successful and Unsuccessful attempts to view/modify/delete audit logs</b></li> </ul>				
<b>Utilize Strong Identification &amp; Authentication leveraging Public Key Infrastructure (PKI).</b>	D	H	CACP-ICT	Customers can implement this requirement within their account, which AWS does not manage on their behalf.

## Document Revisions

Date	Description
May 2017	First publication