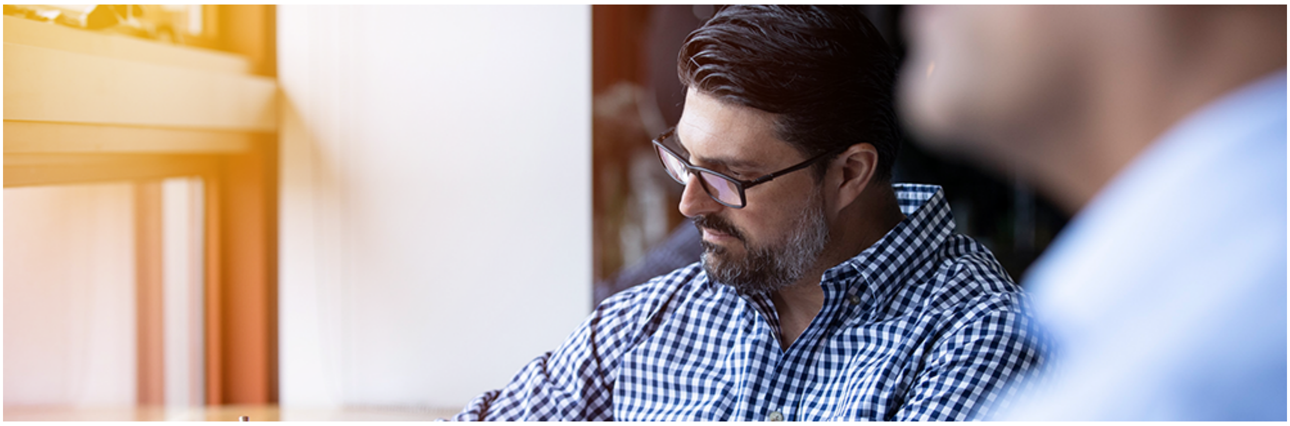
Australian Centre for Advanced Computing and Communication

Acceptable Use Policy



Version 1.1

Table of Contents & Notices

Notices 1

Acceptable Use Policy 2

1. Acceptable use of Services 2
2. Licence Mobility 3
3. AUP applies to all Users 3
4. Changes to AUP 3
5. Usage Limits 3
6. Compliance with Law 3
7. Attacks against Security 4
8. AC3's Enforcement Rights 4
9. AC3's Rights of Suspension or Termination 5
10. Customer Obligations to Report Breaches 6

Notices

The information contained in this document is confidential. It is suitable only for use for its intended purpose and may not be disclosed to third parties.

The contents of this document are not to be copied, reproduced and provided to any other organisation without the express permission of AC3.

Acceptable Use Policy

The information contained in this document sets out the rules and guidelines when using AC3's 'As a Service' and 'Managed Services' including customer obligations, unacceptable uses, changes, usage limits, security measures and the consequences for non-compliance. The AUP is also an integral part of the framework of AC3's information security policies.

1. Acceptable use of Services

a) This Acceptable Use Policy (AUP) describes the conditions when using AC3's As a Service and/or Managed Services ("Services") and the restrictions on that use. The conditions and restrictions described in this AUP are not exhaustive and this AUP may be updated from time to time in accordance with the provisions set out herein.

b) The Customer is solely responsible for:

(i) the content, materials, software and data that the Customer creates, uploads to and processes on AC3's infrastructure;

(ii) the content, materials and data that the Customer creates using the Services; and

(iii) applications and/or software (whether new or existing) that the Customer installs or deploys on AC3's infrastructure (each and together "Customer Content").

c) Any software distributed by AC3 or procured, installed or deployed by the Customer independently (whether new or existing) as part of the Services is subject to the terms of the software licensing agreement provided with the software and any other policy or business requirements deemed necessary by the software publisher, manufacturer or vendor (each and together "Software Vendor"). Where the Customer Content includes new or existing third party propriety software or open source software (each "Third Party Software" – see for example the "Microsoft Licence Mobility" section below) to be installed or deployed by the Customer when using the shared cloud environment forming part of the Services (and such licenses are separate to and independent of AC3's server or other licensing), it is the Customer's responsibility to:

(i) comply with the Software Vendor's verification transfer process to ensure that the Third Party Software licences procured, installed or deployed by the Customer complies with the Software Vendor's licensing requirements; and

(ii) for complying with the terms of each Software Vendor's licence agreement including review and audit requirements and where reasonably requested by AC3 or the Software Vendor reporting usage to, and submitting to audit by, an authorised third party, the Software Vendor or AC3. The Customer agrees that AC3 may submit and charge for licensing usage should an audit or review of the Services (whether by AC3, an authorised third party or the Software Vendor) indicate a discrepancy or misrepresentation by the Customer. Where relevant, AC3 may also pass on to the Customer license cost increases or penalties imposed by AC3 as a result of a breach by the Customer of its obligations as set out in this AUP.

d) All software is subject to the warranties and restrictions (such as return of software), if any, provided by the Software Vendor. The Customer agrees that the Customer and all of the Customer's end-users of the software are bound by, and will abide by, any such software licensing agreements and other requirements notified in advance and in writing to the

Customer or relevant end-user and accepted (including by a ‘click through’) by the Customer or relevant end-user.

e) This AUP applies to all uses of any Services including use resulting from or involving Customer Content.

2. Licence Mobility

a) “License Mobility” is a benefit available to Microsoft Volume Licensing customers with eligible server applications covered by active Microsoft Software Assurance (SA). License Mobility allows customers to move eligible Microsoft software to third party cloud providers where it is a shared environment. It is important to note that Customers may not need license mobility if using their own licenses on private or dedicated cloud environments. To know if a specific product is eligible for License Mobility, Customers should refer to the Microsoft Product Terms. Every product has an individual Software Assurance section that indicates License Mobility eligibility. As at the date of this AUP, License Mobility eligible products include SQL Server, Remote Desktop Services, System Center, Exchange, and SharePoint.

3. AUP applies to all Users

a) This AUP applies to the use of the Services by the Customer’s users, the Customer’s clients or customers, their users, third party service providers and other end-users (Users). As between AC3 and the Customer, the Customer is responsible for the acts and omissions of all its Users.

4. Changes to AUP

a) AC3 may reasonably and lawfully amend this AUP from time to time by posting the updated version of this AUP to the AC3 website or otherwise providing notice to its customers. AC3 agrees that any changes to this AUP from time to time will not materially alter the specifications for the Services as agreed with the Customer, be of material detriment to the Customer’s use of the Services, or result in the Customer incurring any additional costs without first obtaining the Customer’s consent.

5. Usage Limits

a) AC3 has the right to impose limits on any Service made available to the Customer in accordance with the capacity (infrastructure or managed service) it pays for. Under this AUP each Customer agrees to comply with those limits, and further agrees if it, or its Users, exceed those limits AC3 may limit/throttle the Services or impose usage management procedures. Where reasonably possible or practicable for AC3, AC3 will provide the Customer with reasonable prior written notice and a reasonable opportunity to rectify the relevant issue before implementing any such measures.

b) Customers must not circumvent any limits that are placed on any of the rights granted to use the Services, whether usage rights or otherwise.

6. Compliance with Law

a) All Customers and Users must comply with all applicable laws, rules, regulations, industry codes and similar guidelines when using the Services.

b) Without limiting the generality of clause a. above, each Customer or User must not use the Services to:

(i) engage in any illegal business or activity;

(ii) infringe any third party intellectual property right e.g. copyright, patents, trademark, trade secret or know-how;

(iii) collect, copy or process information in a way that breaches privacy or data protection laws;

(iv) distribute, publish, send or facilitate the sending of unsolicited mass e-mail or other messages, promotions, advertising or solicitations in breach of the Spam Act 2003; or

(v) create, distribute, process or view any material that is:

i. defamatory;

ii. obscene, indecent or pornographic;

iii. racist, sexist or otherwise discriminatory;

iv. misleading, deceptive or fraudulent; or

v. other objectionable, offensive or illegal.

7. Attacks against Security

a) No Customer or User may use the Services or allow the Services to be used to:

(i) gain unauthorized access to third party computer systems or networks or engage in attacks against the security of those systems or networks including attacks:

i. against trust such as email spoofing, password cracking, IP spoofing and DNS poisoning;

ii. against confidentiality;

iii. against integrity; or

iv. against availability, such as denial of service;

(ii) corrupt, modify or intercept electronic communications intended for any other person or entity; or

(iii) interfere with or disrupt the operation of the Services or AC3's infrastructure.

8. AC3's Enforcement Rights

a) AC3 may at any time and without notice investigate any suspected breach of this AUP or misuse of the Services.

b) AC3 may block access to Customer Content or remove it from the Services if AC3 has reasonable grounds to suspect that it breaches this AUP. AC3 will notify its Customer(s) of enforcement action taken by AC3.

c) AC3 may, to the extent required by applicable law, cooperate with courts and judicial bodies, police and law enforcement authorities, regulators and other third parties in the investigation and prosecution of illegal conduct using the Services or in the breach of Third Party Software licensing terms. Cooperation may include disclosing information and data about the Services, the Customer, its use of the Services and Customer Content when required by law to do so. To the extent permitted by law and the relevant law enforcement authorities, AC3 will notify its Customer(s) of any cooperative action which affects the Customer(s).

9. Third Party Cloud Services

a) Where the Customer procures Third Party Cloud Services such as AWS and operates within AC3's AWS multi-account structure (with or without AWS Control Tower orchestration):

(i) Identity and access management (IAM) components provisioned for the Customer in order to access the AWS Master (parent) account will have limited administrative privileges. Limited privileges restrict access to services such as: AWS Organizations, general account management, the AWS billing console, AWS control tower administration, AWS cost explorer and AWS budgets.

(ii) The Customer may request full administrative privileges in AWS Organizations linked (child) accounts and can issue such federated (Single Sign-On) roles to staff – however, such child accounts shall have Service Control Policies (SCPs) applied to the limited authorisation of administrative roles and users, to services such as: AWS Organizations, general account management, AWS billing console, AWS cost explorer and AWS budgets.

(iii) Unless otherwise expresly agreed with AC3 in writing, the Customer must not circumvent the authorisations put in place by AC3

b) Unless otherwise expressly agreed with AC3, the Customer is not authorised to perform management of any AWS reserved instances' and savings plans' in any of the AWS Organizations accounts;

c) The Customer may be limited in accessing AWS support features directly in the AWS console for both the master and any child accounts in accordance with the managed services and support agreement in place with AC3.

10. AC3's Rights of Suspension or Termination

a) AC3 may suspend or terminate a Customer's use of the Services if it or its Users materially breach this AUP or misuse the Services.

b) If AC3 decides that the breach can be remedied without suspending access to the Services, AC3 will request the Customer to remedy the breach within the specified time period as notified to the Customer. If the breach is not remedied within that time period, AC3 reserves the right to suspend the Customer's access to the Service.

c) If AC3 suspends access to the Service, and the Customer does not correct the reason for the suspension within seven days of the suspension, AC3 may subsequently terminate the Customer's access to the Service.

11. Customer Obligations to Report Breaches

a) The Customer must promptly notify AC3 if a Customer becomes aware of any breach of this AUP and fully assist AC3 to investigate and remedy the breach.