IT Policy

1 Policy Application

1.1 This policy regulates the use of digital, electronic and information technology resources, including software, hardware, data storage and electronic communication systems and devices (collectively "ACOR IT") utilised throughout the ACOR Group of Companies ("ACOR") in order to:

a) maintain the integrity and security of ACOR IT resources and records;

b) meet ACOR's legal and contractual obligations; and

c) comply with ACOR's quality assurance system and reporting requirements.

1.2 This policy sets out:

a) the standards of behaviour for all ACOR employees, as well as any consultants, independent contractors, labour hire contractors or any other third parties engaged by ACOR ("ACOR IT Users"), who are provided with access to ACOR IT;

b) guidelines regarding the appropriate use of ACOR IT during the course of performing work duties and

c) the accessibility, functions and support systems applying to ACOR IT.

1.3 Where an ACOR employees is provided with access to a client, supplier or third-party information technology network, system or device, in the course of their employment or engagement with ACOR, in addition to complying with this Policy, the employee may be required to comply with the obligations of the owner of the information technology or system. The ACOR employee is to comply with the client, supplier or third-party information technology requirements (insofar as they are not inconsistent with this Policy). If an inconsistency between this ACOR IT Policy and a client supplier or third-party system requirement arises, the employee or ACOR IT User must raise the inconsistency with ACOR IT Services Manager

1.4 This policy is to be read in conjunction with:

a) *Code of Conduct Policy (BSS-POL-NAT-HR001)*;

b) *Privacy Policy (BSS-POL-NAT-HR002)*.

c) *Employee Records Privacy Policy (BSS-POL-NAT-HR003)*; and

d) *Social Media Policy (BSS-POL-NAT-HR021)*;

e) *Equipment Policy (BSS-POL-NAT-HR017)*; and

2 IT Technical Support Function

2.1 ACOR has established an IT technical support function to provide technical assistance for IT related issues ("IT Support") in accordance with *IT Support Procedure (ICT-PRO-NAT-081).*

2.2 Assistance from external IT manufacturers or suppliers (including Microsoft, Apple or other IT providers) is not permitted at first instance or without first referring to ACOR IT Support to seek to resolve the technical issue.

3 IT Supply and Installation

3.1 ACOR provides all employees and approved ACOR IT Users with ACOR IT appropriate to the role (as approved by the applicable ACOR manager) for use during the course of performing work for ACOR. ACOR IT (including type, model, and features) is provided at the discretion of ACOR.

3.2 Any additional ACOR IT (including subscriptions, upgrades, download of additional software or installation of hardware or peripherals to an ACOR IT device) is only to be installed or completed by ACOR IT Support.

3.3 Requests for upgrades, additional hardware or software, subscriptions and access to secure websites ACOR's secured data and files are to be completed in accordance with the *IT Technical Support Procedure (ICT-PRO-NAT-081)*

3.4 Purchase and installation of any unique, non-standard or specialist IT, including hardware or software packages must be approved by an ACOR manager, in accordance with *IT Support Procedure (ICT-PRO-NAT-081),* before being actioned by IT Support.

3.5 Software purchased or licensed to ACOR can only be installed on ACOR IT and must not be used on any external or non-ACOR personal computers

4 IT Access, Usage and Storage

4.1 All employees or approved ACOR IT Users have the responsibility to use ACOR IT and resources in a professional, ethical, and lawful manner.

4.2 Access and Usage of ACOR IT must be in accordance with this Policy. ACOR specific applications, access, storage, and use of ACOR IT shall comply with *Access, Usage and Storage Procedure (ICT-PRO-NAT-080).*

4.3 If an ACOR IT user does not, or refuses to, use ACOR IT in accordance with IT Access, Usage and Storage Procedure, *IT Support ICT-PRO-NAT-081),* ACOR may suspend the user's access to the ACOR IT or decline to provide IT Support.

5 Hardware and Devices

5.1 ACOR IT Hardware and Devices

5.1.1 All ACOR hardware and devices must remain within the care and custody of the assigned ACOR employee or approved ACOR IT User at all times and be stored securely when not in use. Employees and ACOR IT Users must take all reasonable measures to maintain the hardware and devices and prevent loss, theft, damage or destruction of ACOR IT (including when removed from ACOR controlled premises) including storage and transportation using appropriate protective pouches or carry cases.

5.1.2 Employees and ACOR IT Users are required to return ACOR IT in the same condition as provided to them, save for fair wear and tear. Due care shall be taken at all times. Individual staff members will be held liable for loss or damage of property where reasonable precautions were not taken, and the IT hardware or device is damaged as a result.

5.2 Non-ACOR Hardware and Devices

5.2.1 Non-ACOR hardware or devices (including laptops, tablets, external storage, peripherals or networking devices) must not be added to ACOR IT or connected to an ACOR IT network without the approval of IT Support. Before allowing connection of a non-ACOR device or hardware, ACOR IT Support may require the employee or ACOR IT User to:

a) allow an inspection of the device or hardware;

b) conduct a diagnostic or security screening program or allow ACOR IT Support to conduct the action;

c) reformat or reset the device or hardware;

d) install, upgrade or update certain software including security programs;

e) apply a password or other security protocol to the hardware or device.

5.2.2 Private employee or contractor phones, tablets and other devices may be added to the ACOR Guest WIFI portal.

5.3 Mobile Phones, Tablets and other Devices

5.3.1 ACOR may supply an employee or approved ACOR IT User with an ACOR mobile phone. This Policy applies to the use of the ACOR mobile phone as an item of ACOR IT. Incidental personal use that does not conflict or interfere with the employee or approved ACOR IT User's obligations to ACOR including any other ACOR Policy is permitted.

5.3.2 Employees or approved ACOR IT Users are permitted to connect privately owned mobile phones, tablets and devices to ACOR IT networks and secure WiFi as well as install ACOR owned or licensed applications, ACOR email and communication services (including Teams) on the mobile phone, tablet and device.

5.3.3 All appropriate security (including pass codes, automatic locking, facial recognition and encryption) must be applied to prevent unauthorised access or a compromise to ACOR IT occurring.

5.3.4 The Employee or approved ACOR IT User must continue to comply with all ACOR policies, including this Policy, when using the privately owned mobile phone, tablet or device in connection with the performance of work for ACOR.

6 Prohibited Behaviours

6.1 ACOR IT is made available to employees and approved ACOR IT Users for use in the course their employment or engagement.

6.2 Employees and ACOR IT Users must not:

a) breach copyright or any other intellectual property rights belonging to ACOR or any third party. This includes, unless permitted by law or with the permission of the copyright owner, any attempt to:

(i) dissemble source code;

(ii) de-identify ACOR or third-party intellectual property;

(iii) download illegal or unlicensed software; or

(iv) seek to attribute ownership of intellectual property to any person other than the copyright owner.

b) access or install any licensed or secure data using software or applications (including developing software or automation technology) not paid for or approved by ACOR, for the purpose of circumventing or undermining firewalls, encryption or other security protocols;

c) breach any individual's privacy or distribute any information in breach of legal or contractual obligations of confidentiality or privacy, including a breach of *Privacy Policy (BSS-POL-NAT-HR002)*;

d) install, develop, or distribute software or run unknown or unapproved programs on ACOR IT, unless authorised (and under the supervision of) ACOR IT Support in accordance *with IT Support Procedure (ICT-PRO-NAT-081)*;

e) modify software or hardware installed on ACOR IT;

f) obtain unauthorised access (including hacking) into any other computer or device;

g) use ACOR IT:

(i) for personal gain or in furtherance of a personal business or enterprise;

(ii) to participate in online gambling, betting and other games of chance;

(iii) for gaming, streaming platforms for music, television or movies or hosting recreational or entertainment media or digital currency mining;

(iv) to access pornography or websites with adult, violent or abusive themes or to download inappropriate or unlawful images or content;

(v) for storage of personal files or use ACOR IT applications for personal data storage or transfer; or

(vi) to communicate in any other manner that would be in breach of any other ACOR policy including:

- *Social Media Policy (BSS-POL-NAT-HR021)*; or
- *EEO Discrimination Bullying and Harassment (BSS-POL-NAT-HR007)*,

save for incidental personal use that does not conflict or interfere with the employee's obligations to ACOR including any other ACOR Policy;

h) destroy or dispose of ACOR IT or transfer possession to another ACOR employee or third party without authorisation.

7 ACOR IT, Email and Internet Usage

7.1 Employees and ACOR IT Users are entitled to use ACOR IT, email and internet facilities for legitimate business purposes related to their role. Employees and ACOR IT Users must not use ACOR IT, email or internet facilities for personal use if that use interferes with the efficient business operations of ACOR.

7.2 ACOR reserves the right to prevent the delivery of emails sent to or from an ACOR email address, restrict access to an internet website from ACOR IT, if the content is deemed inappropriate for the workplace in accordance with this Policy, or if it is deemed to affect the productivity of ACOR.

7.3 If an employee or ACOR IT User receives an email containing content which is inappropriate for the workplace as set out in this Policy, it must be deleted immediately and not forwarded to any other person.

7.4 Employees and ACOR IT Users must not send (or cause to be sent), transmit, share, upload, download, use, retrieve, store or access any content that:

- is excessive in data size, including streaming of any movies, music or any other media broadcast, and other large amounts of data that is not work related;
- is obscene, offensive defamatory or inappropriate for any person or organisation. This includes text, images, videos, sound or any other material, sent either in an email or in an attachment to an email, or through a link to an Internet site (URL). This may also include material of a sexual, indecent, violent, or pornographic nature or any material that may reasonably offend people due to gender, race, religion, political persuasion or other personal matters;
- causes insult, offence, intimidation or humiliation by reason of unlawful harassment or discrimination to any employee, contractor, supplier or client of ACOR;
- is defamatory to, incurs liability for, or adversely impacts the image of ACOR. A defamatory message or material is a message or material that is insulting or lowers the reputation of a person or group of people;
- is in any way threatening, illegal, malicious, unlawful or inappropriate;
- affects the performance of, or causes damage to ACOR IT and its operation in any way;
- gives the impression of representing, giving opinions or making statements for or on behalf of ACOR without the express authority of ACOR;
- violates any licence or permissions governing the use of ACOR IT including software or websites ordinarily used by ACOR in the conduct of its business;
- transmits any viral or malicious software or self-executing code into ACOR IT or public or private network or device;
- transmits or sends ACOR information, documents or emails (in any format) to any external party or organisation unless expressly authorised by ACOR to do so.

7.5 Employees and ACOR IT Users must not use ACOR IT to:

- create any legal or contractual obligations on behalf of ACOR unless expressly authorised by ACOR;
- disclose any confidential information of ACOR or any customer, client or supplier of ACOR unless expressly authorised by ACOR;
- send or cause to be sent chain, viral or spam emails in any format;
- access and play internet computer games.

7.6 Employees and ACOR IT Users must not subscribe to any non-work-related websites using an ACOR email address.

8 Reporting

8.1 Employees and ACOR IT Users are required to report:

a) any loss, theft, or damage to ACOR IT, device or hardware (including a private mobile phone connected to any ACOR IT) immediately to IT Support (and supply any passwords or information necessary for IT Support to remotely disable, lock or immobilise the ACOR IT or device to protect ACOR's data and information; and

b) any actual or perceived data breach, including exposure to potential phishing, scam, virus or other malicious activity;

c) Report any potential misuse of ACOR IT or a breach of this Policy to their Manager.

9 Expectations of Privacy and Exclusive Use

9.1 Whilst employees and ACOR IT Users are permitted autonomous use of ACOR IT in the course of their employment or engagement (including setting passwords, controlling access to emails, files and data), ACOR retains ownership of all data, files and communications created or received using ACOR IT. Employees and ACOR IT Users do not have a right of exclusive use of ACOR IT. Subject *to Employee Records Privacy Policy (BSS-POL-NAT-HR003)*, ACOR may at any time access or inspect data, files and communications stored on ACOR IT, without the knowledge and/or consent of the employee or the ACOR IT User.

9.2 ACOR IT Support may be requested to provide an ACOR manager with access to an employee's or ACOR IT User's computer, email account or any other files stored on ACOR IT. ACOR would exercise this right of access in limited circumstances including:

a) if the employee or ACOR IT User is away, ill or incapacitated and the information is required urgently;

b) the employee has resigned or no longer employed by ACOR;

c) if the ACOR IT User's engagement is terminated;

d) for the purposes of an investigation arising out of an alleged breach of any ACOR policy, including:

- *Code of Conduct Policy (BSS-POL-NAT-HR001)*;
- *EEO Discrimination Bullying and Harassment Policy (BSS-POL-NAT-HR007)*;
- *Grievance Policy (BSS-POL-NAT-HR008)*;
- *Social Media Policy (BSS-POL-NAT-HR021)*; or
- *Performance Counselling and Disciplinary Policy (BSS-POL-NAT-HR022)*;

e) with the approval of an ACOR manager in circumstances where there is no other reasonably convenient means to locate the information required by ACOR in furtherance of its business and operations.

9.3 ACOR may, but is not required to, inform the employee or ACOR IT User that it proposes to access (or has accessed) the employee's or ACOR IT User's data, files or communications stored on or transmitted using ACOR IT.

10 Security – Passwords, Keys and Encryption

10.1 Employees and or ACOR IT Users must activate and maintain passwords, security keys and encryption to protect ACOR IT in accordance with *IT Access, Usage and Storage Procedure (ICT-PRO-NAT-080)*. The employee or ACOR IT User must disclose the password, key or encryption to ACOR IT Support if required for the purposes of providing technical support, or if directed by an ACOR manager. Any passwords, security keys and encryption applied to ACOR IT by ACOR must not be removed by an employee or ACOR IT User which results in the ACOR IT being insecure or open to access by any third party.

10.2 IT Support may reset or override any password, as required, in order to protect and maintain the integrity and/or security of ACOR IT. All actual, potential or threatened breaches of any password applying to ACOR IT must be reported immediately to IT Support and the employee must follow all instructions and directions of IT Support.

11 Data Backups, Project Archiving and Retrieval

11.1 Digital and electronic files are archived intermittently, at the request of ACOR or at the discretion of, IT Support to manage and maintain the capacity and integrity of ACOR IT.

11.2 ACOR operates backup systems to ensure integrity and reliability of all data stored using ACOR IT. Backup systems will be stored remotely and in multiple locations in order to maximise accessibility in situations involving disaster recovery or other damage or destruction of ACOR's premises.

11.3 It may be possible to restore files that have been inadvertently deleted, overwritten or corrupted. Requests for restoration or retrieval of files should be made to IT Support as soon as possible to maximise the prospects of successful recovery.

12 Cloud Data Storage and Transfers

Digital cloud services are used extensively across ACOR for the saving and transfer of data. ACOR employees and IT Users may only use cloud services approved in accordance with *IT Access and Usage Procedure (ICT-PRO-NAT-080)* for the storage and transmission of ACOR (and client) data.

13 Videoconference Facilities

Videoconference facilities are available to employees and ACOR IT Users for internal and external conferences in accordance with *IT Access and Usage Procedure (ICT-PRO-NAT-080)*. Any other live streaming or video platforms are not permitted to be downloaded or installed on any ACOR IT.

14 Internet, File and Activity Logging

14.1 ACOR reserves the right to log any or all internet activity from, files saved to and activity on its computers and systems. These logs may identify website addresses, file names, file metadata, programs used, actions, time and user details.

14.2 Although ACOR does not have the desire to minutely monitor all activity by its staff members, any such logging would be primarily intended to identify serious breaches of ACOR's policies, as stated in this manual, to allow ACOR to meet its legal and business obligations.

15 Sustainable Energy Use

15.1 Employees are encouraged switch off or shut down computers, devices and any other IT equipment at the end of the day or when not in use. The main reason for switching equipment off is to save energy. It also

allows IT Support to deploy updates when devices are turned back on. IT Support will notify if devices are to be specifically left on to complete an update.

15.2 Computers, devices and monitors account for a large proportion of the electricity used in an office. Energy is being consumed, even by "energy saving" hardware. Otherwise, deploy a “sleep” or “standby” mode to reduce energy requirements when not in use.

15.3 IT equipment produces heat, so turning them off reduces building cooling loads (especially if left on overnight, requiring higher air conditioning requirements at the beginning of the day, when staff are arriving). Though there is a small surge in energy when a computer starts up, this small amount of energy is still less than the energy used when a computer is running for long periods of time.

15.4 ACOR aims to reduce emissions, reduce energy use and reduce environment costs.

16 E-waste

16.1 No ACOR IT may be disposed of or sent for recycling unless approved by IT Support. IT Support will provide instructions for disposal of e-waste to ensure all ACOR confidential information is deleted, all software and data is wiped, and no valuable assets are disposed of.

16.2 ACOR will source an appropriate E-waste donation or recycling provider in the local area.

17 Breach of this policy

17.1 Any employee or ACOR IT User who is found to have breached this Policy (including noncompliance with *IT* Access *and Usage Procedure (ICT-PRO-NAT-080)* or *IT Support Procedure ICT-PRO-NAT-081))* may have access to ACOR IT suspended or cancelled, result in a warning or improvement action or be subject to disciplinary action, including termination of employment. For serious breaches of this Policy, which may also be a breach of legislation, ACOR may refer the breach to law enforcement.