Social Media Policy

1 Introduction

1.1 The purpose of this policy is to outline ACOR Group of Companies ("ACOR") requirements regarding appropriate use of Social Media Applications. It has also been developed to ensure that employees as well as independent contractors and labour hire contractors engaged by ACOR ("contractors") adhere to their obligations to protect Confidential Information and Intellectual Property of ACOR when interacting on Social Media Applications.

1.2 This policy also applies to consultants, subconsultants, contractors and suppliers providing services or goods to ACOR and its clients. It is a shared commitment to uphold this Policy interacting with ACOR and Social Media Applications.

2 Scope

2.1 This policy applies to all employees as well as independent contractors and labour hire contractors engaged by ACOR ("contractors"). Its application is not limited only to use of ACOR provided electronic devices or information systems, on ACOR premises or during standard working hours. It applies to all interactions on any form on Social Media Applications by ACOR employees and contractors.

2.2 This policy also applies, as appropriate, to relationships with customers, clients, vendors and any other business associates of ACOR.

2.3 This Policy supplements, and should be read in conjunction with ACOR's policies in relation to:

a) *Privacy Policy (BSS-POL-NAT-HR002)*;

b) *Grievance Policy (BSS-POL-NAT-HR008)*,

c) *Equal Employment Opportunity ("EEO"), Discrimination, Bullying and Harassment Policy (BSS-POL-NAT-HR007)*; and

d) *IT Policy (BSS-POL-NAT-HR018)*

3 Policy

3.1 ACOR has a legitimate business interest and right to protect its Confidential Information and its reputation. As such, this Policy applies to all information and online communications via Social Media Applications.

4 Social Media Applications

4.1 Social Media Applications include, but are not limited to:

- Social Networking sites e.g. Facebook, Instagram, TikTok, Google Plus, LinkedIn;
- Video and Photo sharing websites e.g. Flickr, YouTube, Vimeo;
- Micro-blogging sites e.g. Twitter;
- Weblogs, including corporate blogs, personal blogs or blogs hosted by traditional media publications, web leads such as RSS feeds;
- Forums and discussion boards such as Whirlpool, Yahoo! Groups or Google Groups;
- Instant messaging services such as Communicator+;
- Online Encyclopaedias such as Wikipedia;
- Any other web sites that allow individual users or companies to use simple direct publishing tools.

4.2 Social Media Applications are also not limited to public websites. This Policy applies to any other electronic application (such as mobile phone based, or handheld/PDA device-based applications including WhatsApp

or Viber) which provide for communication and/or the sharing of information to user groups or the public at large.

4.3 Online communications may include posting or publishing information via Social Media Applications, uploading and/or sharing photos or images, direct messaging, status updates or any other form of interaction and/or communication facilitated by electronic means.

5 Use of Social Media Applications During Work Time

5.1 Employees of ACOR are permitted to use Social Media Applications during work time on a "reasonable use" basis, subject to the provisions of this Policy. Any online communication using ACOR's information systems may be subject to surveillance by ACOR in accordance with its *IT Policy (BSS-POL-NAT-HR018)*.

5.2 Employees and contractors should ensure that their use of Social Media Applications does not interfere with the overall performance of their role.

6 Responsibility

6.1 ACOR employees and contractors must:

a) not disclose any ACOR related information on any Social Media Application unless otherwise authorised by ACOR;

b) ensure that they do not encourage, aid or abet other persons to use Social Media Applications inappropriately or contrary to the requirements of this Policy;

c) ensure they do not disclose any information about other employees on any Social Media Applications;

d) engage in behaviour that is contrary to the requirements of ACOR's *Equal Employment Opportunity ("EEO"), Discrimination, Bullying and Harassment Policy (BSS-POL-NAT-HR007)* and ensure no statement or material is published or disclosed that is obscene, defamatory, threatening, harassing, discriminatory or hateful to any other person, group of persons or entity including ACOR, its officers, directors, employees, agents or representatives, its clients, partners, suppliers, competitors or contractors;

e) ensure they notify their manager, supervisor or an appropriate person within ACOR should they be aware of any material which may damage ACOR or its reputation or be a breach of this Policy;

f) ensure that they do not make any online communication that is in any way disparaging or unfavourable to ACOR, might damage ACOR's reputation, brand image, commercial interests, or the confidence of ACOR's customers and/or is likely to bring ACOR into disrepute or ridicule;

g) maintain and protect ACOR's Confidential Information and not use the name ACOR or any other like title, mark or logo identifying ACOR in any domain name, or in the title of any blog or any other personal site that may be established;

h) not use or display any ACOR or client Intellectual Property in any communications without the express written consent of ACOR.

6.2 Employees or contractors who choose to reveal or imply their place of employment on Social Media Applications or a personal site should be aware that they are potentially increasing exposure for both themselves and ACOR. Employees and contractors are responsible and accountable for information that they put forward on Social Media Applications and should monitor their posts accordingly.

7 Posting on behalf of ACOR

7.1 Employees and contractors are not to post on any Social Media Application on behalf of ACOR without ACOR's written consent.

7.2 ACOR reserves the right to request an employee or contractor to remove any published content which is contrary to the requirements of this Policy.

8 Posting on Private or Personal Social Media Applications

8.1 ACOR recognises that employees and contractors wish to engage and interact about their life and experiences on Social Media Applications, including while at work. ACOR encourages engagement with personal and professional networks on all Social Media Applications about working with ACOR, at ACOR events and workplaces, and on projects for its clients.

8.2 Posting images and information on Social Media Applications creates risks associated with disclosure of personal information as well as geolocation and other metadata embedded with the post or an image and information shared, exposing it to potential abuse and manipulation (including scams, datamining, fraud and, in in the cases of public and defence infrastructure, sovereign risks). ACOR treats the privacy, confidentiality, security and integrity of its employee, its clients, projects and Confidential Information with the highest levels of priority. Before making any post, considerations of whether private, confidential or secure information may be unintentionally or inadvertently shared are required.

8.3 Posts on private or personal Social Media Applications (other than for official or corporate communications approved by ACOR) must:

a) comply with ACOR's policies and not breach this Policy or any of the policies set out in section 2.3 above;

b) if the post includes an image or personal information about any other ACOR employee or contractor, express permission from that person must be obtained before the image or information is shared;

c) not provide information, images, photographs or details about ACOR, a project or client which might be a breach of privacy, confidentiality or security.

8.4 ACOR invites employees or contractors to engage with ACOR before making a post about ACOR, a protect or a client, to enable ACOR to provide any additional support or information.

9 Breach of Policy

9.1 ACOR may require any post on a Social Media Application in breach of this Policy be corrected, clarified or removed by the person or entity making the post.

9.2 An employee or contractor who acts in breach of this Policy may face disciplinary action, up to and including termination.

9.3 In cases where ACOR has incurred costs due to a breach of this Policy, ACOR may seek to recover those costs.

10 Definitions

10.1 "**Confidential Information**" includes but is not limited to information relating to or belonging to ACOR, its customers and clients; customer lists or requirements; suppliers; terms of trade; pricing lists or pricing structures; marketing information and plans; Intellectual Property and other trade secrets; inventions; business plans or dealings; technical data; employees or officers; financial information and plans; designs, reports, templates; product lines; any document identified as being confidential by ACOR; research activities; software and the source code of any such software and any metadata or geospatial information; but does not include information which:

a) is generally available in the public domain; and

b) was known by the employee prior to the disclosure by ACOR.

10.2 "**Intellectual Property**" means all intellectual proprietary rights whether registered or unregistered and whether existing under statute, at common law or in equity throughout the world including, without limitation:

a) all trademarks, trade names, logos, symbols, get up, brand names or similar rights, registered or unregistered designs, patents, copyright, circuit layout rights, trade secrets and the right to have Confidential Information kept confidential; together with

b) any application or right to apply for any of the rights referred to in paragraph (a) above.

10.3 **"Social Media Applications"** is defined in section 4 of this Policy.