INDEPENDENCE GROUP NL: IGO GROUP GOVERNANCE STANDARD 2 – INFORMATION TECHNOLOGY USAGE AND ELECTRONIC COMMUNICATIONS

Original adoption: 27 April 2016

Last review: 26 June 2017

Last amendment: 26 June 2017

1. PURPOSE

Independence Group NL (**IGO**) is committed to providing access to, and use of, technology to improve productivity and efficient communications. However, for corporate governance, security and business continuity reasons, IGO must protect its electronic communication systems and business information from internal and external risks.

2. PERSONS TO WHOM THIS STANDARD APPLIES

The Standard applies to all directors and full-time, part-time and casual employees, contractors and consultants of IGO, and IGO group companies (the **Group**) (each a **User**) and sets out requirements Users must follow when using any hardware or system provided for use, including but not limited to desktop or laptop computers, personal digital assistants, mobile phones, smart phones or other devices connected to Group networks or servers, facsimile machines, email and internet facilities, SMS and Instant Messaging (**IM**) facilities, electronic documents and removable media (such as CDs, DVDs, USBs, portable hard drives and all other portable storage devices), servers, databases, network storage and voice telephony (**Business Systems**) to access or engage with any information or data created, generated, collated, stored and/or used by the Group (**Business Information**).

3. RESPONSIBILITIES

RESPONSIBILITY
Users are responsible for their use of Business Systems and Business Information, including responsibility for advising third parties not to send material which is prohibited by this Standard.
ACCESS TO BUSINESS SYSTEMS AND BUSINESS INFORMATION
Users will be granted network and email access upon the relevant Human Resources or Administration officer completing and submitting an approved commencement form (which is obtained from the IT Helpdesk). Access to the internet and other information services within the IGO network is only permitted through IGO's standard Internet Gateways (as defined by the IT Department) as opposed to dial-up modem, ADSL and Wireless broadband, unless approval is otherwise obtained from the relevant General Manager who will ensure (in conjunction with the IT Department) that

adequate security measures are put in place. Access and use of the internet via an approved medium must be in accordance with the law, this Standard and any other applicable IGO Standard.

Users may only access Business Systems and Business Information when off-site via an IT Department approved access method, which may change from time to time. Users must take adequate steps to secure and protect Business Systems and Business Information off-site. Business Systems and Business Information should not be left where visible or easily accessible e.g. on car seats or in car boots or environments with extreme temperatures.

SECURITY

Do not disclose IGO's Business Information, including photos or videos, unless authorised and disclosed in accordance with IGO's Continuous Disclosure and Information Standard and applicable security standards, and take care at all times to preserve the privacy and confidentiality of Business Information in accordance with the Code of Conduct and relevant employment or service contract with the Group.

An email sent to an address ending in "igo.com.au" is considered secure. Email sent via the internet to other locations is not considered secure and any confidential information should be appropriately secured.

Information that is commercially sensitive or vulnerable, or contains personal or sensitive information (as defined in the *Privacy Act 1988* (Cth)) must be encrypted before transmission across any public network (for example by using a password protected file and a password communicated by telephone, or via an approved file share upload such as Computershare or ASX). Use of a secure file share is appropriate.

Make every effort to ensure that passwords remain confidential, and are not misused, lost or stolen.

Do not permit anyone else to use a User's password and do not disclose a User's password unless authorised.

Change passwords regularly and reasonably disguise any password memory aids.

Do not allow any other employee to access IGO Technology when logged in to a User's username and password, unless that User is supervising their use.

Do not allow an unauthorised third party (such as spouses and children) to access Business Systems or Business Information.

Users may be liable for any actions taken by others using their credentials.

EMAILS AND INSTANT MESSAGING

Identify the sender of external emails and ensure that the standard disclaimer is added to all emails sent from an internal email system.

Clearly state if a statement or offer is not intended to be binding on IGO.

Exercise care when emailing or instant messaging on IGO's behalf. Do not use a personal (or other) email or IM account when conducting business on IGO's behalf.

Do not enable automatic forwarding of emails to personal accounts (or vice versa) without the IT Department's approval.

Before a planned period of absence, place an out of office message via Outlook and, where appropriate, delegate authority to relevant files and email mailboxes.

INFORMATION MANAGEMENT

Store all Business Information on the IGO network rather than on local drives.

Manage data and delete outdated or superseded electronic documents regularly.

Ensure that data is encrypted and/or moved to the network.

Unsubscribe from unwanted mailing lists to reduce the amount of "Junk" emails in the network.

Do not delete any electronic document that the IGO Legal Department specifies is not to be deleted until a release notice is issued by the Legal Department.

All incoming and outgoing emails are automatically archived and stored for a period of ten years from date the email is sent or received.

SOFTWARE

Users may only use licenced software authorised by the IT Department.

The use of shareware or freeware software is not permitted unless it has been approved and installed by the IT Department.

PERSONAL EQUIPMENT

Do not connect personally owned equipment to any part of IGO's internal network unless approved by the IT Department. Refer to the IT Asset Management Guideline.

The IT Department will not provide support or services for personally owned computer hardware or software. Advice may be sought from the IT Department in respect of suitable computer service repair providers for personally owned equipment.

PERSONAL USE

Users of Business Systems may use email and internet access for limited and reasonable personal use, provided it does not interfere with work practices or performance, and complies with this Standard, other applicable IGO Standards and applicable laws.

Accessing social networking sites (such as Facebook or LinkedIn) or other non-work related sites using Business Systems is only permitted during lunch breaks and personal time provided it does not interfere with Users duties. Access is governed by the IGO Social Media Standard and can be removed at IGO's discretion.

Users access personal financial data from Business Systems at their own risk. The Group accepts no liability or responsibility for the security or protection of the data.

Users must not store non-work related data within Business Systems, particularly large video, picture and audio files.

UNACCEPTABLE USE
While using Business Systems, do not: • engage in any activity that is illegal (including but not limited to any breach of laws regarding privacy, copyright, human rights, equal opportunity, harassment, discrimination, intellectual property and occupational health and safety) or without appropriate regard to privacy, rights and reasonable sensitivities of other people; • send, access, copy and/or knowingly receive materials on the internet or by email that is, or may be, prohibited by any applicable law, including (but not limited to) pornographic, obscene or objectionable material; material portraying violence, nudity or inappropriate content; gambling websites; abusive defamatory or offensive material; false or misleading material; material intended to annoy, harass or intimidate another person; and/or material which may infringe copyright law; **Note:** Users who participate in circulating such material are in breach of this Standard, regardless of whether the User received the material unsolicited; or • fail to maintain professional standards when communicating internally or externally, by, for example, using profanities, abusive or threatening language or making derogatory or discriminatory comments.

4. MONITORING

IGO will monitor and audit Business Systems to ensure that Users are complying with this Standard. A User consents to IGO monitoring and auditing their conduct by using Business Systems. Any records of User access to, and use of, Business Systems may be accessed, viewed, recorded, copied, used, disclosed, modified or destroyed at IGO's discretion. To the extent permitted by law, Users do not have a right of privacy to personnel information stored in Business Systems.

The IT Department will monitor the use of non-work related sites and will report to departmental managers if deemed excessive to ensure compliance with this Standard.

The IT Department will regularly review files stored within Business Systems and may, at its discretion, move or delete suspected non-business related files.

IGO scans all incoming and outgoing emails, electronic documents stored on the network and local hard drives for viruses. Generally, viruses will be cleaned and removed immediately. If a virus cannot be cleaned, the document containing the virus will be automatically deleted.

5. REPORTING A BREACH

If a User becomes aware of a breach of this Standard, or receives or views any messages, comments, correspondence or images that are inappropriate, they should address the individual concerned directly and refer them to this Standard, and report the matter to their manager or the HR Department.

A breach of this Standard is considered serious and may result in disciplinary action, including termination of employment or contract, as set out in the IGO Counselling and Discipline Procedure.

If you have any questions, concerns or feedback about this Standard, you should contact the Company Secretary at: Independence Group NL, PO Box 496, South Perth, WA 6151.

Phone: 08 9238 8300

Email: contact@igo.com.au, Attention: the Company Secretary

This Standard will be reviewed annually by the Board.

***