GROUP GOVERNANCE STANDARD 3 PRIVACY STANDARD

DATE: 8 JULY 2019

DATE	CHANGE	APPROVED
08/07/2019	Addition of Appendix 1: IGO Protocol for Data Security Breach and cross referenced in section 3.5.	
24/6/2019	Last amendment	Board
24/6/2019	Last review	Board
23/1/2015	Original adoption	Board

TABLE OF CONTENTS

1. PURPOSE

IGO Limited (**IGO** or the **Company**) and IGO group companies (the Group) are committed to respecting the privacy of Personal Information of any individuals who deal with IGO. "Personal Information" is information or an opinion about an individual or an individual who is reasonably identifiable, whether true or not and whether recorded in material form or not.

2. PERSONS TO WHOM THIS STANDARD APPLIES

This Standard applies to all directors, and full-time, part-time and casual employees of the Group and any other individual that IGO may collect personal information from.

3. RESPONSIBILITIES

3.1 Application of privacy laws

IGO is bound by the Australian Privacy Principles under the Privacy Act 1988 (Cth) (as amended or superseded) and other applicable Commonwealth and State laws which protect privacy. Any permitted handling of Personal Information under exemptions under these laws will take priority over this Standard to the extent of any inconsistency.

3.2 Personal information collected

IGO only collects Personal Information that is necessary for its functions and activities.

IGO may collect Personal Information from a customer, agent, supplier, contractor, adviser, financier, joint venture partner or business partner, an employee of the above mentioned entities, or an individual who contacts IGO, uses the IGO website or applies for securities. IGO may also collect other Personal Information for the purposes of matters connected with its relationship with a person or their employer, including, but not limited to, providing information on services, carrying out transactions and engaging under commercial terms. IGO may also collect Personal Information if you work for or with IGO, for payroll, superannuation, health and safety, administration, security, insurance, staff management and contact purposes. If an individual applies for a position with IGO, it may collect information about experience, character, qualifications and medical conditions, and do screening checks. IGO collect, use and disclose Personal Information to assess an application, conduct screening checks and contact someone about other positions. In certain circumstances IGO may collect sensitive information such as criminal record and medical information with consent or otherwise in accordance with the law.

Generally, IGO tries to collect Personal Information directly, however, there are certain situations in which it may collect personal information indirectly. In either case, IGO will take reasonable steps to ensure the person is aware of the purposes for which the information is collected.

Email alerts: IGO ensures subscribers to email alerts are aware of the IGO privacy statement prior to subscribing. When third parties subscribe to IGO's email alert service, IGO records their e-mail address.

Cookies: Users of the IGO website should be aware that cookies may be stored on their computer ("computers" includes personal computers, laptops, smart tablets and smart phones). A 'cookie' is a short text file that may be stored on a computer when a website is visited. When a third party accesses or views IGO's website, the third party is made aware that a cookie may be downloaded to their computer by an external company that provides share price details and charts for the IGO website. These cookies do not collect or track any personal data or information about individuals, however may be used by IGO to review how its website is used so that IGO may enhance the accessibility of its website. IGO will not use cookies or other tracking data to circulate advertising or promotional material.

3.3 Use and disclosure of personal information

IGO will generally use and disclose Personal Information for purposes related to the main purpose for which the information was collected, or where there is consent to the use or disclosure or where required or authorised by law or court order, which may include emergency situations and assisting law enforcement agencies.

When third parties subscribe to IGO's email alert service, IGO will only use their email address for the purpose it has been provided, not add the email address to a mailing list (unless specifically requested) and not disclose the email address without the third party's consent.

IGO may provide Personal Information to contractors and service providers, including organisations that assist IGO with archival, auditing, accounting, customer contact, legal, business consulting, banking, payment, debt collection, delivery, data processing, data analysis, information broking, research, investigation, insurance, website or technology services, Government authorities, regulators, advisers, printers, mail house and registries and where required by law, policy or the rules of a securities exchange, and in the case of staff, to health service providers and other representatives including unions and legal advisers and parties involved in the purchase or potential purchase of all or part of IGO's business. Some of these third parties may be located in other countries in which IGO operates. While those third parties will often be subject to confidentiality or privacy obligations, they may not always follow the particular requirements or procedures under Australian privacy laws. However, IGO will take reasonable steps to ensure that any overseas third party recipient handles the personal information in a way that generally complies with Australian privacy laws.

3.4 Accessing and updating personal information

IGO takes reasonable steps to make sure that the Personal Information it collects, uses and discloses is accurate, complete and up-to-date.

To make a request to access or correct any Personal Information IGO holds, or to raise any privacy concerns, please use the contact details below. IGO asks that as much detail as possible is provided with a request and notes that IGO may need to verify the identity of someone making a request. IGO may not be required by law to provide access or to correct Personal Information. If that is the case, reasons for that decision will be given.

3.5 Security of personal information

Irrespective of whether Personal Information is stored electronically or in hard copy form, IGO takes reasonable steps (see Appendix 1) to protect the Personal Information from misuse, loss, destruction, unauthorised access, modification or disclosure. As far as permissible under the law, IGO accepts no responsibility for unauthorised access to personal information held by IGO.

If you have any questions, concerns or feedback about this Standard, you should contact the Company Secretary at: IGO Limited, PO Box 496, South Perth, WA 6951.

Phone: 08 9238 8300 Email: contact@igo.com.au, Attention: the Company Secretary

This Standard will be reviewed annually by the IGO Board of Directors to check that it is operating effectively and whether any changes are required.

APPENDIX 1: IGO PROTOCOL FOR RESPONDING TO DATA SECURITY BREACHES

IGO protocol for responding to data security breaches

(in conformance with the Australia Privacy Principles [APPs])

IGO has an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known data breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that IGO holds. Includes unintended disclosure of confidential information by IGO personnel or third parties.

Contain

The first step is to **contain** a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

Assess

Consideration must be given to whether or not the data breach is likely to result in serious harm to any of the individuals whose information was involved. If we have reasonable grounds to believe this is the case, then IGO must notify the affected individuals, the Privacy Commissioner and other relevant authorities (see review). If we only suspect that this is the case, then we must conduct a risk assessment. As part of the risk assessment, consideration must be given to remedial action where possible.

The risk assessment must specifically include the following steps:

- Initiate: plan the risk assessment and assign a team or person to complete the task
- Investigate: gather relevant information about the incident to determine what has occurred
- Evaluate: make an evidence-based decision about whether serious harm is likely. The risk assessment must be documented.

The risk assessment must be completed expeditiously and, where possible, within 30 days. If it can't be done within 30 days, we are obliged in law to document why this is the case. 'Serious harm' is defined as the release of data, that in the assessment of a 'reasonable person', could credibly result in serious physical, psychological, emotional, financial, or reputational harm.

Immediate remedial action

Where possible, steps must be taken to reduce any potential harm to individuals. This includes notifying them of the data breach.
Next action must be taken to recover lost information, if possible, or change access controls before unauthorised transactions can occur. If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.

No — **Is serious harm Likely?** — **Yes**

Notify Authorities

Where serious harm is likely, IGO must prepare a statement for the Privacy Commissioner (a form is available on the Commissioner's website) that contains:

- IGO's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals

IGO must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:

- Option 1: Notify all individuals
- Option 2: Notify only those individuals at risk of serious harm. If neither of these options are practicable:
- Option 3: A statement must be published on IGO's website and publicised

Consideration must be given to making an apology and providing an explanation of what IGO is doing about the breach.

Review

Review the incident and take action to prevent future breaches. This may include:

- Fully investigating the cause of the breach
- Developing a prevention plan
- Conducting audits to ensure the plan is implemented
- Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices

Consideration must be given to reporting the incident to other relevant bodies, such as:

- police or law enforcement
- ASIC, APRA or the ATO
- The Australian Cyber Security Centre
- professional bodies
- IGO's financial services provider(s)

Note: Where IGO is operating in jurisdictions outside of Australia, we may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.

For further information refer to : www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response#is-serious-harm-likely