Christie Vazquez, Shahla Raei, Janet Mai, Yee Ann Chen, Mai Ta

ACCEPTABLE USE POLICY

1 SUMMARY

1.1 Purpose

1.1.1 This policy provides direction on appropriate use to protect OAS IT assets and information.

2 APPLICABILITY

2.1 Scope

2.1.1 OAS and its operating companies are referred to herein, collectively, as "OAS." Applicable local laws, regulations, and other restrictions will apply in the event of any conflict with this document.

3 POLICY

3.1 Asset Ownership

3.1.1 IT Asset Owners will be identified for all OAS IT assets. These owners will identify the IT assets under their control and ensure that the protection provided corresponds to the business value of the asset.

3.1.2 IT Asset Owners will authorize access to the assets under their control.

a. Allowing any member of the public or any unauthorized users to Access Company IT assets is prohibited.

b. Access by competent law enforcement personnel may be granted only with appropriate legal authority (subpoena, search warrant, or during customs inspection), as determined by the OAS Legal.

3.1.3 IT Asset Owners are to review and confirm appropriate user access at least annually for assets containing proprietary information (e.g. private, restricted), and a host high or medium impact applications.

3.2 Acceptable Use of IT Assets

3.2.1 IT assets will only be used for authorized business purposes. However, incidental and infrequent personal use is acceptable. To the extent limited by applicable law OAS has the right to monitor the use of IT assets.

3.2.2 Only computer systems provided by OAS or its designated IT support suppliers are allowed to connect to the OAS network.

3.2.3 No personal computers are allowed to connect to the OAS network.

3.2.4 Connecting non-standard mobile devices to the OAS network is prohibited.

3.2.5 USB ports on all IT assets must be disabled for the use of portable storage media (e.g., USB memory sticks, external hard disk drives, etc.).

3.3 Securing and Storing Information

3.3.1 OAS computer systems used to store or present company information to employees or third parties must be secured to OAS IT standard.

3.3.2 Critical business data must always be managed in such a way that at least one copy is always stored on an OAS server.

3.4 Labeling and Handling Information

3.4.1 OAS proprietary information must neither be stored on personally-owned devices nor on devices other

than those issued by OAS or its authorized IT support supplier.

3.4.2 Computer hard drives and other media containing proprietary information, and\or licensed software (including network devices, printers and multi-function scanning/printing devices) must be processed before leaving the control of OAS in order to protect OAS information.

3.4.3 Proprietary information and technical data will not be posted on any computer system accessible to the general public or accessible on the general OAS intranet unless protected by further restrictions.

3.4.4 Telecommuters are responsible for protecting proprietary information in a manner commensurate with its sensitivity, value, and criticality.

3.4.5 The use of technologies such as search engines or "crawlers" must only be implemented in accordance with this policy.

4 EXCEPTIONS

4.1 OAS IT Risk Exception Request

4.1.1 OAS Workforce members who cannot abide by any OAS IT policies, standards, or procedures must request a security risk exception by following the *OAS IT Risk Exception Procedure*.

4.1.2 Exceptions to enable USB ports for portable storage media may be requested by using the USB Exception form and has an expiration of one year.

5 ENFORCEMENT

5.1 Non-Compliance Warning

5.1.1 OAS Workforce members found violating any OAS IT policies, standards, or procedures may be subject to disciplinary action, up to and including termination of employment and/or legal action.