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

CONTROLS FOR ACCEPTABLE USAGE POLICY

1 OBJECTIVES

1.1.1 Ensure that IT security policies exist and provide adequate requirements for the security of the environment.

1.1.2 Determine how those policies are communicated and how compliance is monitored and enforced.

2 VERIFY ADEQUATE POLICY COVERAGE

2.1 **Acceptable usage of the company's information assets by employees (for example, whether employees can use their computers, the Internet, and e-mail for personal reasons)**

2.1.1 Role-based access for emails and downloads from the internet.

2.1.2 Security controls on installing devices and/or software on any personal computers or workstations assigned to them by the company.

2.1.3 Administrative controls on security awareness and training programs, information ownership, disposal of IT assets and supervision.

2.1.4 IT assets controls on hardware and software inventory, information asset register.

2.2 **Passwords**

2.2.1 Password structure: Passwords must be changed every 4 months and be at least 8 characters in length, and contain a mix of uppercase, lowercase, numbers and special characters and cannot contain the employee's personal.

2.2.2 Password display: Passwords must not be displayed on the data entry/display device.

2.2.3 Password disabling: Additional measures, such as disabling, renaming or decoying these standard accounts, should be employed.

2.2.4 Password changes control: Each web user should periodically be prompted to change his or her password. The interval between password changes could be at 30, 60, or 90 days, etc. which is set at the level of the organization.

2.2.5 Storing of passwords: Passwords must be stored in irreversible encrypted form and the password file cannot be viewed in unencrypted form.

2.3 **Data classification, retention, and destruction**

2.3.1 Requirements and standards on data classification for OAS and clients information.

2.3.2 Controls on data retention and destruction of IT assets that store OAS and clients information.

2.3.3 Input, processing and output controls including accuracy and validation of data, and completeness of outputs.

2.4 **Remote connectivity**

2.4.1 Overall network security and security requirements for virtual private network (VPN), dial-up, and other forms of connection to external parties (granting of remote connectivity, lost and stolen protocol).

2.5 **Server security**

2.5.1 Audit trail log file controls.

2.5.2 Security controls for back-up, disaster recovery and business continuity, physical security and use of storage media.

2.6 **Client security**

2.6.1 Security requirements for desktops and laptops (physical locks, removing, installing of security applications).

2.7 **Logical access**

2.7.1 Segregation of duties and privileged access.

2.7.2 Administrative controls on personnel management.

2.7.3 Requirements for obtaining and granting access to systems.

3 VERIFY STAKEHOLDER BUY-IN

3.1.1 Ensure that key stakeholders were included during policy creation.

4 VERIFY PROCESSES AROUND THE POLICIES

4.1.1 Review processes for periodically reviewing and updating the policies to ensure that they keep up with the ever-changing IT environment.

4.1.2 Review processes for periodically evaluating changes in the environment that might necessitate the development of new policies.

4.1.3 Ensure that provisions have been made for obtaining approved exemptions from the policy.