INFORMATION TECHNOLOGY POLICY

NETWORK PROJECT

Man Kit Kwan

Table of Contents

INFORMATION TECHNOLOGY SECURITY POLICY

1 INTRUCTION

a. This Policy applies to all information contained on the Internet and business functions, the physical environment and relevant people including all staff, contractors, and visitors.

b. The transmission of information across networks and the Internet increases the company's risk of exposure to accidental, or deliberate, unauthorised modification or disclosure. Adherence to this policy will ensure that our Information Systems (IS) are developed, operated, used and maintained in a safe and secure manner.

c. The network is a collection of communication equipment such as servers, computers, printers, routers, switches, and firewalls, which has been connected together by cables or wireless devices.

2 ACCEPTABLE USE POLICY

ACCEPTABLE USE

The types of activities that staff, contractors and visitors are encouraged to participate in and considered acceptable practice when using Information System systems include:

a. Research on the Internet related to develop professional skills related to develop professional skills related to one's position at Optimus Consultant.

b. Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.

c. Reasonable use of computing facilities for personal correspondence, e.g. sending personal emails, and using Internet so long as it does not interfere with productivity or consume sustained high-volume traffic.

UNACCEPTABLE USE

The types of activities that are considered unacceptable practice include:

a. Use of equipment and Internet services for illegal or unlawful purposes. This includes, but is not limited to: intentional copyright infringements, software license infringements, obscenity, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation and computer tampering (e.g. spreading computer viruses or destruction of data owned by others).

b. Intentionally using equipment and Internet services to visit Internet sites or receive information that contains obscene, pornographic, hateful or other objectionable material.

c. Attempting to gain access to any computer system, information, or resources without the authorisation of the relevant owner.

d. Knowingly or recklessly transmit or distribute any information or material which contains a virus, worm, Trojan Horse, or any other harmful component.

e. Posting, publishing, transmitting, or distributing any unsolicited advertising through mass electronic- mail or other direct transmission.

f. Using digital technology and Internet services to reveal or publicise restricted or propriety information which includes, but is not limited to: financial information, new product ideas, intellectual property, strategies and plans, databases and the information contained therein, staff details, product information, computer software and code, computer network and access details and business relationships.

g. Internet use of a nature that consumes bandwidth at an unacceptable rate is specifically prohibited when there is no clear educational use. Examples include: illegal downloading of music, video or software; playing games online.

All use must comply with all applicable laws which include but is not limited to: the Privacy Act 1993, the Fair Trading Act 1986, the Copyright Act 1994, the Defamation Act 1992 and the Films, Videos, and Publications Classification Act 1993, the Unsolicited Electronic Messages Act 2007 as well as any advertising codes of practice which may be relevant.

3 ACCESS CONTROL POLICY

This defines the security practices that control access to information and computer systems at Optimus Consultant. The following apply:

a. Only Optimus Consultant staff and authorised visitors are allowed to access and use the Information System services.

b. User accounts are to be created and managed by Information Technology Maintenance Department, this includes:

   - The creation and deletion of all user accounts.
   - Periodic auditing of accounts to verify account status.
   - Unlocking accounts that have been locked by security features.
   - Deleting accounts that have been disabled for a period longer than 6 months unless specifically authorised to remain disabled.

c. Information System accounts can be immediately disabled at the request of Administration Department.

4 PASSWORD MANAGEMENT POLICY

a. Passwords must be kept confidential and are the responsibility of the individual. They are not to be shared or used by anyone else, even for a short period of time.

b. Password construction must comply with the following minimum standards:

- All passwords are required to be a minimum length of 8 characters.
- Password construction must include a combination of uppercase, lowercase, numbers and symbols where possible, and not contain a complete word including a person or company's name.
- Passwords will be changed every 60 days.
- Login attempts will be restricted on all IS services after 5 unsuccessful login attempts; account will be locked

5 REMOTE ACCESS POLICY

Remote access to Optimus Consultant Information System Services is provided for staff to work from home and access services remotely, for example remote access to Share Folders. The following apply:

a. Remote access is only permitted through Management Department approved; contact the Information Technology Maintenance Department for guidance on the remote access services available.

6 APPLICATION AND SOFTWARE POLICY

This defines the security practices when developing, integrating or installing new software and what needs to be considered during the acquisition or evaluation of new software. The following apply:

a. Only approved software is to be installed on Company devices. Non-approved software that is installed will not be supported by Information System staff and may be removed.

b. All shareware software must be licensed to Optimus Consultant.

c. No software is to be installed when there are insufficient licenses available.