HONG KONG AERO ENGINE SERVICES LIMITED

INFORMATION SECURITY POLICY

Document Control

Document Name	HAESL INFORMATION SECURITY POLICY
Version Number	2.6
Prepared by	IT team
Publish Date	27 Feb, 2024

1. SECURITY AWARENESS AND TRAINING

BACKGROUND

Management and employees should be reminded of their information security responsibilities regularly and should be provided with security awareness training at least once a year to be able to assist the company in securing its assets and to enable the employees to fulfill their information security responsibilities.

DETAIL

a. HR Department will incorporate the Information Security Policy into the Code of Conduct induction training for all employees at the commencement of employment.

b. For any updates on the Policy, Function Heads will be responsible for delivering the changes in the departmental briefing.

c. The refresher training on Code of Conduct (inclusive of this Policy) will be held on a regular basis.

2. COMMUNICATION WITH EXTERNAL PARTIES

BACKGROUND

Sensitive information should only be disclosed outside of the company to parties that are authorized to receive such information.

DETAIL

a. Employees should take care of what information to disclose when communicating with outside parties. Considerations include what they are authorized to disclose and the risk of potential impact to the company.

b. Any communication of Internal and Sensitive information to outside parties must be approved by the respective information owners.

c. A confidentiality agreement is mandatory when Internal and Sensitive information is to be exchanged with third parties as part of a contractual relationship. If a contract is not in place when discussing potential projects with outside suppliers, then considerations must be given to the use of a non-disclosure agreement.

d. Sensitive information should be encrypted, or password protected where appropriate before sending.

3. PHYSICAL ACCESS

BACKGROUND

Physical access of staff and visitors in the company must be managed and controlled to minimize the risk of Sensitive information being accessed or removed from the site by any unauthorized individual.

DETAIL

a. All visitors to the site must be registered; the registration process must be able to confirm the identity of the person visiting, the organization he or she represents, the purpose of visit and details of the person whom the visitor is meeting.

b. Respective Function Heads are responsible for securing areas with Sensitive information. Additional physical security measures commensurate with the areas' higher risk levels should be considered.

c. Function Heads are responsible for authorizing appropriate physical access required for all regular and temporary employees within their respective areas of management, and access should be granted to only those areas and times appropriate for normal working arrangement.

d. Where practical, keep the minimum possible amount of paper and electronic media on desk during working hours; store all papers and physical media with Sensitive information in locked storage while not in use or after office hours.

4. ELECTRONIC MAIL AND INSTANT MESSAGING

BACKGROUND

Sensitive information should only be sent through the company's authorized electronic messaging system.

DETAIL

a. Use of any alternative electronic messaging system other than the corporate authorized electronic system for exchanging company information is not allowed.

b. Employees must NOT:

- Send messages to large groups unless there is a specific business requirement.
- Forward unofficial chain messages.
- Allow other users to use their user account.
- Auto-forward e-mails on the corporate e-mail system to a private e-mail account.
- Auto-forward e-mails to another employee' s account unless there is a specific business reason.

c. Create or distribute any disruptive or offensive messages or use inappropriate language which would compromise the company brand.

d. All file attachments must be scanned with the company's anti-virus/malware program prior to them being opened.

e. The corporate messaging system is monitored to detect suspicious activity and log files are maintained for potential investigation purpose.

5. INTERNET USAGE

BACKGROUND

To avoid information security related risks or disclosure of Sensitive information without proper authorization, additional care must be taken when using internet facilities.

DETAIL

a. Personnel accessing the Internet are prohibited from conducting inappropriate activities, including but not limited to the following:

- Transmitting any Sensitive information without proper authorization and not through an authorized channel;
- Posting personal opinions concerning Sensitive information on the Internet;
- Producing, posting or sending illegal or offensive messages or material including anything that may defame, embarrass, threaten, harass, offend or harm an employee, service provider, customer or anyone else;
- Visiting malicious websites which may post security threats to the company;
- Downloading material which infringes other company’ s intellectual property rights, copyright, or which is unethical or malicious;
- Initiating and perpetuating “chain” style correspondence; and
- Downloading unauthorized computer software or applications.

b. The company reserves the right to restrict individual or group access to any Internet site it deems necessary.

c. Internet access logs are enabled and maintained for potential investigation purposes.

6. COMPUTERS AND IT EQUIPMENT

BACKGROUND

All computers (whether workstations, laptops and/or other IT equipment) should be properly secured from unauthorized access or misuse of information.

DETAIL

a. Users must not install networking facilities into the company's network without prior approval from IT Department. Such facilities include but are not limited to modems, wireless access points, Internet access or other external network connections that could allow external parties to gain access to the company systems and/or networks and information.

b. Users must not install any type of software (whether the software is copy-protected, no-copy protected, shareware or freeware from removable media, the Internet, email or other software transportation medium) into the company computers and network facilities.

c. Screensaver passwords must be installed to prevent unauthorized access to computer when away from desk.

d. Encryption software or password protection should be provided in the application to protect Sensitive information.

e. For physical security, laptop computers must be secured whilst unattended.

f. Changes to application configurations, application programs, operating systems and network, should be properly documented, including changes to the security requirements, should be approved by respective "system owners" for implementation, and must be properly tested by appropriate personnel prior to being moved to production. The IT Department accountable for establishing proper security controls and procedures for application and infrastructure development, implementation and maintenance.

g. Access requests to systems should be reviewed for compliance with the company's relevant policies to ensure access rights are granted according to job responsibilities with proper segregation of duties, approved by authorized individuals, entered accurately into the system, and reviewed annually for continued compliance.

7. SOCIAL MEDIA

GENERAL

1. Hong Kong Aero Engine Services Limited ("HAESL") recognize that social media has changed the way information is shared and can, appropriately used, be an effective and efficient communication tool. This social media policy (the "Policy") provides guidance on the appropriate use of social media. HAESL supports open dialogue and recognizes the opportunities which social media can provide. HAESL does not want to stop people from using social media. But social media can harm HAESL and its employees financially and reputationally. This is particularly so when a user is identified as an employee of or as otherwise connected with HAESL. The aim of the Policy is to protect HAESL and its employees from such harm.

2. The Policy applies to all employees of HAESL and to temporary workers, consultants and others similarly engaged in connection with HAESL business ("Users"). All Users in Hong Kong must comply with the Policy. Users outside Hong Kong must comply to the extent possible, having regard to local legal requirements and policies.

3. Users must not breach HAESL's code of conduct or its respect in the workplace, whistleblowing, personal data, diversity and inclusion, information and cybersecurity and other policies. Users should be respectful to others when using social media.

4. The Policy applies to the use of social media for personal as well as business purposes, outside as well as during office hours and to the use of personal as well HAESL devices and equipment. It applies to all social media, present and future, including Yammer, Twitter, Facebook, LinkedIn, TikTok, Instagram, Snapchat, WhatsApp, WeChat, Wikipedia, TripAdvisor, YouTube, Flickr and LIHKG.

FUNCTION HEADS

5. Function heads must ensure that Users in their departments are aware of the Policy and are given appropriate support and information, including any necessary additional guidelines specifically applicable to their departments.

USERS

6. All Users must:
   a. understand and adhere to the Policy;
   b. only post on social media information which is accurate and lawful; and
   c. report misuse of social media to their heads of department.

USE OF SOCIAL MEDIA

7. All use of social media on behalf of HAESL must be authorized in writing by HAESL. This includes maintaining an account for HAESL, posting messages and comments for HAESL, uploading content and responding to others for HAESL.

8. Personal use of social media must comply with the Policy. Users are personally responsible for what they put on social media. Users must not post unprofessional or inappropriate content and must not use social media in a way which conflicts with responsibilities to HAESL.

9. Users who identify themselves as HAESL employees or post material related to their work must make it clear that any opinions are theirs alone and not those of HAESL. The following disclaimer must be used. “The postings on this site are my own and do not necessarily represent the views and positions of my employer.”.

SPECIFIC RULES

10. Users must keep their social media accounts secure (for example by regularly changing passwords and using passwords which are sufficiently complex), to prevent unauthorized access.

11. Users must not post:

    a. anything which may cause damage to HAESL’s reputation, bring HAESL into disrepute or be otherwise against the interests of HAESL.

    b. defamatory or adverse statements or comments about anybody (including other employees in HAESL and customers and suppliers of HAESL and including offensive, derogatory, discriminatory, harassing, bullying and threatening statements and comments).

    c. inappropriate images or links to inappropriate content.

    d. HAESL trademarks or logos or references to HAESL brands, unless so authorized.

    e. private or confidential information, trade secrets or proprietary information (whether or not belonging to or related to what they do for HAESL and including non-public information about the businesses of HAESL and its financial performance).

REPORTING NEGATIVE POSTS

12. If you come across negative or disparaging content about HAESL or its businesses on social media do not react yourself. Send the content to your head of department, who will decide what to do about it.

COMPLAINTS AND INVESTIGATIONS

13. Users who wish to report misuse of social media (including a breach of the Policy by other Users) or who consider that they have been bullied or harassed through social media may complain to their heads of department or by using the mechanism in the HAESL whistleblowing policy.

14. When a complaint is received or a suspected breach of the Policy is reported, the relevant function head will conduct a preliminary inquiry to determine whether there are sufficient grounds for further investigation. If there are such grounds the function heads will inform Human Resource Manager. Human Resource Manager will, after consulting others as appropriate, appoint an investigator to conduct the further investigation.

15. Investigators will report their findings and recommendations to the Human Resource Manager and the relevant function head, who will, after consulting others as appropriate, decide what to do, including taking disciplinary action.

DISCIPLINARY ACTION

16. Breaches of the Policy may lead to disciplinary action. Users may be required to remove social media content. Failure to do so may itself result in disciplinary action. Serious breaches of the Policy (for example posting material which causes serious financial or reputational harm to HAESL or any of its employees) may constitute serious misconduct and may lead to summary dismissal. HAESL may also take action to recover any loss or damage it may suffer.

RIGHT OF AMENDMENT

17. HAESL reserves the right to amend any provision of this Policy from time to time.

8. REMOTE ACCESS

DETAIL

Only authorized persons may remotely access the Company network. Remote access is provided to those employees, contractors and business partners of the Company that have a legitimate business need to exchange information, copy files or programs, access computer applications or provide remote support services.
Users should follow the Remote Access policy to access the resources that are kept on office network through remote access:

a. Login with Two-factor authentications
b. Use company provided devices is recommended
c. For using owned devices, ensure up-to-date antivirus and definition, software patches are installed
d. Remote connections to the company's network must be timed out after a period of inactivity defined by the Company (e.g. 15 minutes).
e. Connect via Remote PC or App

9. PERSONNEL OUTSIDE OF OFFICE

DETAIL

Internal, Sensitive and Highly Sensitive information should be handled securely by users when they are away from office, including but not limited to during overseas travels.
During travel, users should:

a. Lock all Internal, Sensitive and Highly Sensitive information (in paper form or on electronic equipment) when it is not being carried in person.
b. Do not leave any Internal, Sensitive and Highly Sensitive information (in paper form or on electronic equipment) in an unattended vehicle or a hotel room whilst unattended (unless it is locked in a safe cabinet or any similar secured storage location)
c. Avoid discussing Sensitive and Highly Sensitive information in public areas. If discussion of Sensitive and Highly Sensitive information in public places cannot be avoided, employees should use guarded terms and refrain from mentioning sensitive details unless necessary.
d. Position the equipment screen such that unauthorized persons cannot readily look over their shoulder and see what is on the screen.
e. Dispose the Internal, Sensitive and Highly Sensitive information concerned upon returning to the office if secure disposal is not possible whilst offsite.
f. Use Remote PC or App. software to access the resources that are kept on office network through remote access where necessary.