HONG KONG AERO ENGINE SERVICES LIMITED

INFORMATION SECURITY POLICY

Version: 2.2

Publish Date: 01 Apr 2021

The policy content is originated from HAESL - Information Technology Department. If you have any queries or suggestion for this manual, please do not hesitate to contact this originator.

HAESL INFORMATION SECURITY POLICY

CONTENTS LIST

1. INFORMATION SECURITY (IS) ROLES AND RESPONSIBILITIES

BACKGROUND

Information security is an integrated function that requires effective organization and coordination. Roles and responsibilities are important in HAESL.

DETAIL

a. General Manager Finance & Administration (GMFA) is responsible for providing leadership in the area of information security, formulating information security standards and procedures for the company and monitoring compliance with the Policy and the Guidelines.

b. Information Owners (Function Heads unless otherwise noted) are responsible for ensuring that their respective information assets have been properly protected.

c. The IT Department is responsible for providing and maintaining a secure IT environment which hosts the company's information systems and digital information.

d. All company personnel are responsible for taking all necessary precautions to protect the information they come in contact with, including but not limited to

- Taking steps to restrict access to information on a need-to-have basis;
- Keeping strong passwords confidential and changing them on a regular basis;
- Not posting sensitive company or customer information on social media, instant messaging networks, non-company email systems or other similar sites;
- Ensuring that sensitive information is not left unattended on office desks;
- Using encryption to prevent disclosure of confidential electronic information;
- Immediately reporting security incidents;
- Securing their personal computer environment and mobile devices; and
- Securing sensitive printed documents.

e. The Human Resources Department is accountable for ensuring that all new employees have acknowledged the IS Policy and the Guidelines at the commencement of their employment and to maintain on-going training.

f. The IT department must ensure that all access to IT systems (for example email and mobile device management) is revoked when employee leave.

g. All employees should be required to remove promptly ex-employees from all business-related communication groups (for example WhatsApp and WeChat).

2. INFORMATION LIFE CYCLE MANAGEMENT

BACKGROUND

All employees must be capable of identifying information that is sensitive, assessing potential risks to the company, and applying appropriate classification and protection.

DETAIL

1. Information Owner

- The Informational Owner is responsible for ensuring the proper implementation of the information classification scheme and associated controls within their respective areas of management.
- The Information Owner is required to identify, risk analyze, classify and protect sensitive information and data used for the purpose of conducting company business irrespective of the medium on which it resides and regardless of format.
- The Information Owner is required to monitor compliance with the Policy and ensure protection levels for information within their respective areas of management.

2. Protection

a. Protection of all information shall be implemented according to Confidentiality, Integrity and Availability.

3. Confidentiality

a. Information shall only be accessible to relevant employee and authorized non-employees on a need-basis.

b. Where required non-disclosure agreements shall be implemented in employment, customer and supplier contracts.

c. Non-disclosure agreements shall be executed between HAESL and business partners before exchanging Internal and sensitive information.

d. For Sensitive information, it must be encrypted for transmission, for example Payroll data is always stored with encryption by software.

4. Integrity

a. In respect of HAESL policies and procedures, any changes must be recorded (e.g. EPM amendment). At a minimum, who and when for the change must be documented.

b. For Public and Sensitive information, detection of unauthorized change shall be implemented with appropriate means – including procedural and/or technological where fit.

5. Availability

Retention

The information being kept during the retention period (e.g. Engine Dossier) shall be provided to the authorized parties only.

Backup and Restore

The information shall be backed up according to the business requirements defined by the information owners. The backup shall be coordinated by IT and no standalone backups are allowed (e.g. portable hard drives).

6. Classification

There should be at least four classifications of information:

a. Public - Non-sensitive information available for public disclosure.

b. Internal use only - Information belonging to the business unit not for disclosure to the public or external parties, but generally available to employees and authorised non-employees.

c. Sensitive – Information that is sensitive or confidential within the business unit and intended for business use only by those who need to know it without unreasonable compromise of accessibility or integrity.

d. Highly sensitive – Information that is extremely sensitive or private, of the highest value to the business unit and intended for use by named individuals only without unreasonable compromise of accessibility or integrity.

3. 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.

4. 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.

5. PHYSICAL ACCESS

BACKGROUND

Physical access of staff and visitors in the company must be managed and controlled in order 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.

6. MOBILE PHONES AND OTHER PORTABLE MOBILE DEVICES

BACKGROUND

Mobile devices that contain Sensitive company information and/or can access corporate networks must be properly protected from unauthorized information leakage.

DETAIL

a. Mobile devices are subjected to the same restriction on information security relating to the access and use of company information as non-mobile devices.

b. Company supplied mobile devices, and personal mobile devices accessing the company network or storing company Sensitive information

- must be configured to protect against unauthorized disclosure of information in accordance with company security standards;
- must be configured with strong password standards;
- must be configured with mobile device management (MDM);
- must be enabled with remote data wiping.

c. Employees must not attempt to by-pass or remove the company security policy configuration on device holding company data.

d. Employees are responsible for removing any company Sensitive information from their mobile devices or relocating such information to a more secure storage once it has been read or used for the intended purpose, and before disposal of the device.

e. Employees should immediately report to the IT Department any incident or suspected incident of unauthorized use of or access to mobile devices which possess company Sensitive information, a remote wipe command (if supported by the device) should be sent to the mobile device to remove company data.

7. 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.

8. 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.

9. 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.

10. REQUIRED PRACTICES RELATING TO THE INTERNET OF THINGS (IOT)

BACKGROUND

IoT are sensors or devices connected to a network, for example meter sensors, CCTVs and Signage TVs. They are usually less secure than normal computer equipment. The following should be done in order to improve their security:

DETAIL

a. Establish network visibility and controls over them;

b. Change their default accounts and passwords;

c. Connect them to networks which are segregated from business units' normal computer networks;

d. Adjust their configurations and turn off unnecessary features (e.g. voice control on Signage TVs);

e. Any custom software development relating to IoT should be done having regard to the Open Web Application Security Project (OWASP) IoT security Guideline; and

f. Test and apply security patches in a timely manner.

Data created from IoT must be capable of being managed dynamically.

11. REQUIRED PRACTICES RELATING TO PERSONAL DATA

DETAIL

- Referring to Human Resource EPM Volume (04-11-07-01).

12. REQUIRED PRACTICES RELATING TO OUTSOURCED SERVICES

DETAIL

- Referring to Material Management EPM Section 10 of Volume 40.

13. 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), in order 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 authorised;

    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 a 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.

14. SECURITY INCIDENT DETECTION, ESCALATION AND RESPONSE

BACKGROUND

Once detected, all breaches of confidential company information must be reported, responded to and escalated in a timely manner.

DETAIL

a. Employees have a duty to report as soon as possible any information security breach in relation to Sensitive information of which they become aware to the information owner. All reported incidents must also be reported to the IT Department.
b. Employees must not release any security incident details to external parties without the consent of Senior Management.

15. INVESTIGATIONS

DETAIL

The IT Department is responsible for conducting investigations for all reported incidents to determine cause and to identify and implement corrective actions, in order that security can be continuously refined and enhanced. When an investigation is required, it is extremely important that evidence is collected, retained, preserved and presented in a way that conforms to the rules for the collection of evidence.

16. REVIEWING, AUDITING AND MONITORING

DETAIL

The IT Department is responsible for ensuring this document is reviewed on an annual basis. The QA Department is responsible for audit and compliance monitoring.

17. REQUIRED PRACTICES RELATING TO THE TRANSPORTATION OF SENSITIVE INFORMATION

DETAIL

Referring to Material Management EPM Section 10 of Volume 40.

18. REQUIRED PRACTICES RELATING TO CONFIDENTIAL WASTE

DETAIL

Referring to Material Management EPM Section 10 of Volume 40.

19. 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 at a period of inactivity defined by the Company (e.g. 15 minutes);
e. Connect via Remote PC or App

20. 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.

21. REMOVABLE STORAGE DEVICES

BACKGROUND

Removable Storage Devices – e.g. external hard disk, removable SSD, USB memory stick, mobile devices with storage cards and internal memory such as digital cameras, IOT devices or mobile phones, etc.

DETAIL

Attaching removable storage devices to the corporate IT network introduces cybersecurity risks such as data leakage and malware infection. Whenever practicable, sharing Company files and data through removable storage devices should be prohibited and enforced technically.

Company supplied devices (i.e. Laptops, PCs) must have their interface ports (i.e. USB or Firewire) disabled for connecting removable storage devices. Securer alternatives or Company storage solutions should be used for sharing files internally and externally.

Alternatives for common business usages:

Scenario	Business usage	Alternatives
#1	Internal Work file Save /Copy /Transfer /Sharing	Using Company storage solutions. (e.g. Microsoft OneDrive/ Teams Storage / SharePoint, or Network Shared folders.
#2	External Work files sharing	Using securer alternatives. (e.g. encrypted Email, password protected attachment, SFTP, Company OneDrive etc.).