ASIA HOUSE

HOME OF BUSINESS - CULTURE - PEOPLE

IT Security Policy for The East Asiatic Company Foundation and Asia House

Content

Public IT Security Policy for The East Asiatic Company Foundation and Asia House

1. SCOPE

This policy constitutes the overall framework for information security in the EAC Foundation and Asia House, both for the EAC Foundation and Asia House as a company, as well as in all the EAC Foundation and Asia House's deliveries to customers.

INTRODUCTION AND PURPOSE

The purpose of information security in the EAC Foundation and Asia House is:

- To protect confidentiality, integrity and availability of information and information systems. By this we mean:
  - **Confidentiality** - Ensure that access to information is provided only to persons with the proper authorization.
  - **Integrity** - Ensure that information is correct and has not been changed or manipulated in any way, whether inadvertently or intentionally.
  - **Accessibility -** Ensure that information and information systems are available within the stipulated framework and agreements.
- To ensure that the EAC Foundation and Asia House comply at all times with applicable laws and regulations, as well as contractual requirements.
- That the EAC Foundation and Asia House work with information security to support the companies' business models, financial performance, and the EAC Foundation and Asia House's credibility to the outside world, including collaborators, customers and authorities.
- To ensure that technical or procedure-based controls implemented in the companies The EAC Foundation and Asia House, are based on an effective risk assessment.
- To maintain the EAC Foundation and Asia House's reputation as trusted and trustworthy suppliers.

ROLES AND RESPONSIBILITIES

The following roles and responsibilities have been defined:

Role	Responsibility
Management	The management of the EAC Foundation and Asia House is responsible for setting the guidelines for compliance with the laws relating to personal data.
Employees	Are expected, in their daily work, to comply with the policies and procedures set by the EAC Foundation and Asia House regarding the processing of personal data.

SCOPE AND VALIDITY

This Information Security Policy shall apply to:

A. Any information the EAC Foundation and/or Asia House owns, may be held responsible for or treat, regardless of the form in which it is stored or conveyed. This applies regardless of the technological platform used for storage and processing.

B. All EAC Foundation and Asia House employees, temporary employees, collaborators and consultants, service providers, subcontractors and their employees.

C. In all outsourcing relationships where access or use is made of EAC Foundation and Asia House information and systems.

COMPLIANCE

The management of EAC Foundation and Asia House commit themselves to ensuring continuous improvement of the information security management system.

THE COMPANY'S SAFETY PRINCIPLES

The EAC Foundation and Asia House's work depend on the safe handling of information in both electronic and physical form. For this reason, information security is an integral part of the company's business security.

MAINTENANCE OF COMPETENCIES

The EAC Foundation and Asia House maintain and supports the level of knowledge of all employees to secure the safe processing of information in the company's information systems. This is done by continuous training of the company's employees.

CREDIBILITY

In the event that external parties are affected by security incidents at The EAC Foundation and Asia House, the companies will communicate honestly and trustworthily to affected parties.

2. DETECTION AND HANDLING OF SECURITY INCIDENTS

The EAC Foundation and Asia House have established a clear process for handling security incident, with the purpose of ensuring that the company responds appropriately to actual or suspected security incidents concerning information systems and data. Examples of such security incidents could be illegal intrusion, compromise of systems, misuse of information and information resources and breach of the continuity of critical information systems and processes.

3. ACCESS

Access to resources and applications is approved by the respective system owner. Recertification of users' access to the respective systems happens bi-annually. This is carried out by the system owner.

Unauthorized access:
Users of the EAC Foundation and Asia House’s Information Resources must refrain from attempting to obtain, or allow others to gain, unauthorized access to the systems. It is the user's duty to report any deviation from the policies and procedures to the responsible person.

Remote access:
Remote access to the EAC Foundation and Asia House’s IT Infrastructure may only be attempted using a secure remote application or portable facilities provided by the EAC Foundation or Asia House. Remote access to administrative and production networks is not possible.

User-assigned usernames and passwords:
Users can only access computer systems by using an authorized username and password. Users may not use usernames or passwords other than their own to access the EAC Foundation and Asia House’s computer systems. In addition, users should not deliberately allow the use of their username and password by others, regardless of whether such a person is an authorized user or not. Users are also advised that they are responsible for all work stored or retrieved, messages sent or received, or transactions performed via the Internet under their username and password, in cases where appropriate measures to protect the confidentiality of these credentials have not been taken.

The user's username and password cannot be reused for other internet services such as LinkedIn, Facebook or similar.

The user's password is changed continuously every 90 days. Users generate a password of at least 8 characters. The user's last four passwords are remembered by the system so that they cannot be reused.

Access to unauthorized networks/service:
Users may not access, or attempt to access, networks, network drives, or archives and folders for which the user has no legitimate reason to access, regardless of whether the user is entitled to do it or not (need-to-know).

4. CONTINGENCY PLAN

The EAC Foundation and Asia House have established a contingency plan, which ensures that the company's business processes are protected against the impact of major errors in information systems or disasters, thereby ensuring a timely recovery of the affected services and protection of company employees.

5. SUPPLIER MANAGEMENT

The EAC Foundation and Asia House shall maintain appropriate levels of information security and service delivery in accordance with agreements with third parties.

Delivery of services:
The service provided by third parties should include security measures, service definitions and service management agreements.

Third Party Services Monitoring and Auditing:
Third party services, reports and records must be monitored and reviewed on a regular basis.
Data processing agreements with suppliers are obtained. Additionally, annual audits of these suppliers are conducted.

In practice, this will be done by obtaining a third party statement of assurance from the suppliers.

6. USER TRAINING

All EAC Foundation and Asia House employees' awareness of IT security-related topics should be strengthened on a regular basis. Education and information are important for IT security and the safety-driven behavior of the end-user. The **management** determines which training is appropriate for the members of staff who have access to confidential information, based on a risk vs. cost assessment.

7. BREACH OF THE COMPANIES' SAFETY REGULATIONS

Breaches of the EAC Foundation and Asia House Security Regulations may result in sanctions against employees, in accordance with staff policy. In relation to collaborators, suppliers and their employees, the penalty will be in accordance with the terms provided in the relevant service agreements.

8. FOLLOW-UP AND APPROVAL

This security policy is reviewed annually, or when major changes in the overall risk picture occur, in relation to the Companies' overall business strategy or in the organization.

This policy has been approved and revised by management.

2. DOCUMENT INFORMATION AND REVISIONS

Document information:

Location: Public

Document author: Signe Weber Carlsen

Document responsible: Susanne Rumohr Hækkerup

Approved by: Chairman of the Board, Erik Bøgh Christensen

Version	Date of commencement	Text / revisions	Who	Document name
1.0	25.05.2018	New document.	SWC	IT Security Policy v.05.2018