AEON Credit Service (Asia) Co., Ltd.
Statement on Information Security

Table of Contents

1. **Purpose** 3
2. **Scope** 3
3. **Information Security Principles** 3
4. **Continuous Improvement and Management Oversight** 4
5. **Roles and Responsibilities** 4
6. **Data Protection and Information Integrity** 4
7. **Monitoring of Information Security Threats** 5
8. **Information Security Incident Management** 5
9. **Supplier Relationships and Third-Party Information Security** 6
10. **Business Continuity and Resilience** 6
11. **Compliance and Review** 7

1. Purpose

AEON Credit Service (Asia) Company Limited ("ACSA" or the "Company") is committed to protecting its information assets, customer data and information systems. This statement outlines ACSA's commitment to managing information security risks, maintaining the integrity and protection of data, monitoring and responding to information security threats, and continuously improving its information security management.

2. Scope

This statement applies to ACSA's operations. It is intended to serve management, IT administrators, system owners and information security stakeholders, who have the responsibility to assess the security impact in embracing various computing models for the storage, processing, or transmission of classified data in ACSA.

In addition, this statement is intended as reference for vendors, contractors, and consultants who provide IT services to ACSA.

3. Information Security Principles

ACSA is committed to maintaining the confidentiality, integrity and availability of information.

ACSA will ensure that:

- Customers' personal data will be protected against any unauthorized or accidental access, processing, erasure or other use.
- Confidentiality of customer data will be preserved;
- Integrity of information will be maintained;
- Availability of information to support business processes will be assured;
- Availability of customer data for access and correction by customers.
- Regulatory and legislative requirements such as Personal Data (Privacy) Ordinance are complied with.
- IT Aspect of Business Continuity Management is developed, tested and put in place.
- Information security trainings are available to all employees.
- Procedures for preventing, detecting, investigating and reporting information security breaches are in place.
- Appropriate procedures are devised and implemented to support this statement.

4. Continuous Improvement and Management Oversight

Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

Through regular review and enhancement, ACSA seeks to continuously improve its information security policies, procedures, controls and systems in response to changes in business operations, technology, regulatory requirements and the information security threat environment.

5. Roles and Responsibilities

Management shall require all employees and external party users to apply security in accordance with established policies and procedures of ACSA.

Management shall ensure that appropriate information security roles and responsibilities are defined, assigned, and supported to effectively manage and operate security controls, safeguard information assets, and address cyber security risks.

ACSA shall provide appropriate awareness education and training to all employees and relevant contractors to do their job properly and securely.

Employees and contractors using ACSA’s information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.

6. Data Protection and Information Integrity

ACSA is committed to ensuring the integrity and protection of data throughout its lifecycle, including collection, processing, storage, transmission, retention and disposal.

Appropriate controls are applied according to the value, criticality and sensitivity of information to safeguard information against unauthorized access, disclosure, alteration, or misuse. These controls include, but are not limited to, access control, secure data handling, system protection, backup, monitoring, and secure disposal measures, and supporting the protection of intellectual property rights.

7. Monitoring of Information Security Threats

Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.

Information relating to information security and cyber security threats shall be systematically collected and analyzed to produce relevant and actionable threat intelligence. This intelligence shall be used to support the implementation and continuous improvement of security controls to prevent, detect, and respond to cyber attacks, thereby strengthening ACSA's overall cyber security resilience.

Information about technical vulnerabilities of information systems being used shall be obtained promptly, ACSA's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

8. Information Security Incident Management

Management shall establish responsibilities and procedures to ensure a quick, effective and orderly response to weaknesses, events and security incidents.

Information security incidents and events shall be reported through suitable management channels as soon as practicable.

Information security events shall be assessed and then it can be decided if they should be classified as information security incidents, events or weaknesses.

Information security incidents shall be responded to in accordance with the documented procedures.

Knowledge gained from analysing and resolving information security incidents shall be used to help reduce the likelihood or impact of any future incidents.

9. Supplier Relationships and Third-Party Information Security

Information security requirements for mitigating the risks associated with supplier's access to ACSA's assets shall be agreed upon with the supplier and documented.

All relevant information security requirements shall be in place with each supplier that has access to or can impact ACSA's information, or assets that process it.

Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

ACSA shall regularly monitor, review and audit their supplier service delivery.

Any changes in the services provisioned by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed.

10. Business Continuity and Resilience

ACSA shall determine its requirements for information security and the continuity of information security management in adverse situations.

ACSA shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during a disruptive situation.

ACSA shall verify the established and implemented information security continuity controls regularly to ensure they are valid and effective during these situations.

Information processing facilities shall be implemented with redundancy sufficiency to meet availability requirements.

11. Compliance and Review

ACSA complies with applicable laws, regulations and contractual obligations relating to information security, privacy and data protection. The Company reviews related information security policies and arrangements periodically and updates them where necessary to reflect changes in business needs, regulatory expectations, technology and the information security risk environment.

Last update: 25 August 2026