ACCA SOFTWARE

INFORMATION SECURITY POLICY

INTRODUCTION

The spread of ICT technologies at all levels of society entails an increase in security risks in terms of data loss, intrusions, loss of confidentiality and breaches of privacy, and this applies in particular to information systems, thus requiring a careful analysis of their weaknesses and the possibilities of their insecure use. The implementation of an adequate information protection system is based on a systematic analysis of possible threats, and the determination of the precautions to be taken. In the remainder of this document, ACCA refers to this Business Unit.

REGULATORY REFERENCES

ISO/IEC 27000	Information Technology - Security Techniques - Information Security Management Systems - Overview and vocabulary
ISO/IEC 27001	Information Technology - Security Techniques - Information Security Management Systems - Requirements
ISO/IEC 27002	Information Technology - Security Techniques - Code of practice for Information Security Management
ISO/IEC 27017	Information Technology - Security Techniques - Code of practice for Information Security Controls based on ISO/IEC 27002 for cloud services
ISO/IEC 27018	Information Technology - Security Techniques - Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors

POLICIES

GENERALITY

ACCA software S.p.a. is in charge of the following mission:

Design, development, distribution and support of software application packages. Organisation and delivery of training courses, multimedia training aids and e-learning, in the construction sector. Design, development and provision of on-line and on-web applications and services. Creation and management of technical and regulatory databases.

ACCA therefore processes public and confidential data, anonymous, common or sensitive personal data, including highly critical data. They also include personnel and privacy data.

Given the potentially critical nature of the data processed, in whatever format they are (computerised or otherwise), it is essential that they are guaranteed maximum confidentiality, integrity and availability.

The levels of security to be guaranteed must be such as to comply with contractual clauses and current legislation, as well as the consistency and balance between:

- Enterprise risk
- Economic sustainability
- Results of analyses and risk assessments
- Company policies, codes of conduct and strategies towards employees, customers and suppliers

ACCA's policies, already defined as part of the Management Systems for Quality, the Environment and Occupational Health and Safety, are focused on the constant adaptation of the context in which it operates and on improving the effectiveness and efficiency of processes, performance and safety controls.

Listed below are the various key principles on which this policy is based:

- Compliance with legal requirements, technical standards and contractual safety requirements of information.
- Information must be accessible only to those who need it (*need-to-know* principle) and on time.
- Staff must be appropriately involved and trained in information security, and must follow prescribed and agreed ethical and behavioural principles.
- Suppliers must be properly monitored; relations between ACCA and supplier companies of products and services must be based on a contractual framework that takes into account the expectations of both parties and the clear definition of commercial agreements, timeframes and technical and organisational requirements and responsibilities, including those relating to the protection of information.
- The nature of the services provided already requires consideration of security requirements right from the negotiation with customers.

The ultimate responsibility for information security lies with the Management, which delegates the Managers to implement what is necessary, and according to specific Organigrams, in agreement with the IT Systems Manager and the Human Resources Manager.

Although *governance is* delegated to several functions, the management retains responsibility for providing strategic direction and supplying the necessary resources.

ACCA SOFTWARE

COMMUNICATION AND POLICY REVIEW

ACCA Software's management defines, discloses and is committed to ensuring that this Information Security Management Policy is understood and maintained. Disclosure may be by posting on a notice board or by publication on the company intranet.

It is intended to guarantee the safeguarding and protection against threats, whether of internal or external origin, of an accidental or intentional nature, to which information is subjected in the context of activities falling within the scope of the Management System, in accordance with the ISO/IEC 27001 standard and the guidelines of the ISO/IEC 27002 standard.

The Policy must be applied at all levels in the company, and must be part of the agreements that the company enters into with any internal or external party that is involved in the handling of information that falls within the scope of the Management System. To this end, this Policy must also be communicated, when necessary, to external parties (Customers, Suppliers, Supervisory and Control Bodies) interested in the secure management of information.

The information security policy is reviewed at least annually for adequacy, and updated if necessary.

In particular, the updating of the Policy and Operating Practices is indispensable where the Management Review identifies:

- Significant business developments
- New threats compared to those considered in the risk analysis activity
- Significant security incidents
- New requirements and pressures from target markets
- Developments in the regulatory or legislative environment for secure information processing

In particular, the company's activities are based on the assumption of a secure and properly functioning ICT system. Almost all information is stored and processed in electronic format. ICT assets are not immune to vulnerabilities, so it is necessary to carry out a detailed cataloguing of IT assets, as well as planning and control of their security.

The ICT Security Strategy is divided into the following areas:

- Organisational aspects of ICT Security (organisation, personnel)
- Infrastructure security (e.g. data centres, IDF rooms)
- Security of ICT physical media (e.g. servers, clients, network components)

- Network security (network and system management)
- Account Management, i.e. proper Access Management
- Security in applications (e.g. E-Mail, etc.)

INFORMATION SECURITY MANAGEMENT SYSTEM

The starting point for defining the requirements of an Information Security Management System is to identify the possible threats present. Threats are on the one hand dependent on the operating environment, and on the other hand on the sensitivity of the information being managed.

They can be divided into different types of events:

1) Unauthorised modification of information (loss of Integrity)
2) Unauthorised access to information (loss of Confidentiality)
3) Unplanned or unauthorised impacts on the functionality of the System (loss of Availability)
4) Information from unreliable sources (loss of Authenticity)
5) Loss of control over personal data (loss of privacy)

Proper management of information, particularly information on computer media, is a basic condition for guaranteeing and maintaining the set objectives of Integrity, Confidentiality, Availability, Authenticity and Privacy of Information.

Failure to meet adequate security levels leads to very negative consequences:

- Damage to corporate image
- Lack of customer satisfaction
- Penalties for non-compliance
- Leakage of sensitive information and know-how from the company
- Economic and financial damage

The rules, procedures, organisational arrangements and responsibilities defined to achieve the objectives of Integrity, Confidentiality, Availability, Authenticity and Privacy of Information form the basis of the Management System implemented by the company.

To identify security needs, the company periodically assesses risks in order to determine the level of exposure of information to the various threats present. The results of this assessment determine the actions to be taken, the controls and the security measures to be adopted.

ACCA SOFTWARE

INFORMATION SECURITY POLICY OBJECTIVES

1) Acquire full knowledge and awareness of the information managed and assess its criticality, in order to determine and implement appropriate levels of protection.
2) Create a cataloguing of the company's assets relevant to information management, identifying, for each of them, a person in charge.
3) Classifying information on the basis of certain levels of criticality.
4) Ensure secure access to information, according to certain authorisation matrices, in order to prevent access by those who do not have the necessary rights.
5) Granting access to company premises and individual premises only to Authorised Personnel, in order to protect the security of the company premises and assets therein.
6) Define procedures for the secure use of company assets and information, including security aspects also in all phases of design, development, operation, maintenance, support and decommissioning of IT systems and services.
7) Implement a system of collaboration and awareness between the organisation and interested third parties, so that information is treated at appropriate security levels.
8) Promptly recognise Incidents and Faults, including those concerning Information Systems, managing them according to procedure and implementing appropriate prevention systems.
9) Ensure compliance with legal requirements and fulfilment of security commitments set out in contracts with third parties.
10) Ensure Corporate Business Continuity and Disaster Recovery, through the adoption and implementation of appropriate security procedures.
11) Ensuring the confidentiality, integrity and availability of data stored, accessed and manipulated using cloud computing services.
12) Establish a framework of responsibilities and actions needed to meet regulatory requirements and security guidelines for cloud computing.