



**Microsoft**  
GOLD CERTIFIED  
**Partner**

Learning Solutions  
Information Worker Solutions  
Advanced Infrastructure Solutions  
Networking Infrastructure Solutions



**SOPHOS**  
Silver Partner



# Information Security Policy

Version: 01

Type: Final

Level of classification: Public use

Date: 08 – 05 – 2009

Procedure code: C0 – 4

## **Information Security Management System Policy**

(ISO 9001:2008 – 4.2.1 b), 5.3 refers)

### **1. Introduction**

**CACTTUS** has adopted a set of policies and procedures that reflects its commitment to information security. These policies are reviewed annually, on a Management Review Meeting.

This Information Security Policy applies to all **CACTTUS** information assets and demonstrates the commitment given to security assurance and the efforts being made to comply with best professional security standards.

The purpose of the Information Security Policy is to protect our information assets from all threats, whether internal or external, deliberate or accidental. Through the Information Security Policy, the controls and supporting policies, we aim to ensure confidentiality, integrity and availability of Information at **CACTTUS** at all times.

An assessment of the security measures required to protect the assets has been conducted as part of the Risk management process and has been documented in the Risk Assessment Report and the Risk Treatment Plan. This includes business domain risk assessment according to ISO 27005:2005.

*Through this policy we, at **CACTTUS**, as well show compliance with the applicable legal requirements.*

### **2. Our Business**

**CACTTUS** is the leading Kosovar company in the field of system integration, consultancy, implementation, support and training of modern and adaptable IT infrastructure offering services to both private and public sector organizations, but as well to organizations seeking to work with these sectors.

Our existing and prospective client base demands a high quality output and ultimately our business depends on providing our clients with good quality advice and continuous support.

The commitment we undertake in this policy statement therefore reflects the nature of our business.

### **3. Statement of Intent**

It is the policy of **CACTTUS** to apply effective and appropriate information security set of controls, which may be policies, practices, procedures, organizational functions and software functions. And all of them will be aligned with the Cactus business strategy and objectives.

The Company's policies on information security are supported by its other policies relating to quality assurance and the company's commitment to continuing professional development and training for its employees.

Our approach to information security includes both technical and non-technical controls, and covers all eleven aspects of Information Security. In all cases **CACTTUS** will seek the client's approval of use of sensitive client's information as defined in our contracts.

**CACTTUS** will ensure that the following requirements are met:

- Information is **protected against unauthorized access**
- **Confidentiality** of information is assured
- **Integrity** of information and service is maintained
- **Availability** of information and service is maintained
- **Authentication** ensures only authorized user access
- **Regulatory and legislative** requirements are met
- **Contractual security** obligations are considered

- **Business Continuity plans** are produced and maintained to support this policy
- **Information security training** is available to all staff
- **All breaches of information security**, actual or suspected, are reported to, and investigated by the **Quality and Information Security Manager (QISM)**.
- Appropriate action for consequences of **IS policy violations**.

Specific policies and controls that support it are documented in the **CACTUS' QISMS MANUAL** and in the [Statement of Applicability](#).

#### 4. Responsibilities

##### The Managing Partners

- ✓ Hold ultimate responsibility for the Information Security Management System and approves the Information Security Policy. Ensures adherence to the Information Security Policy, as well as its review and communication to all staff.
- ✓ Hold responsibility for the continuous improvement of the effectiveness of the Information Security Management System through the Information Security Policy, security objectives, audit results, monitored events, corrective and preventive actions and the management review.
- ✓ Hold responsibility for providing the necessary recourses for implementation and maintenance of the Information Security Management System  
Review the policy on regular intervals to ensure appropriateness

##### Information Security Manager

- ✓ Holds responsibility for continuous improvement of the effectiveness of the Information Security Management System
- ✓ Holds direct responsibility for maintaining the Information Security Management System, Information Security Policy and giving directions for its implementation
- ✓ Holds responsibility for ensuring effective implementation of the Information security policies, but holds the right to delegate that responsibility to a competent employee
- ✓ Holds ultimate responsibility for managing the information security incidents and reporting those incidents to the Managing partners

##### All Employees

- ✓ Hold responsibility for implementation of this Information Security Policy
- ✓ Hold responsibility to ensure implementation of applicable Information Security Controls to provide for the integrity, availability and confidentiality of Information Resources.
- ✓ Hold responsibility for reporting security incidents.

Lulëzon Jagxhiu  
Managing Director

Date  
8/5/2009