General Information Security Policy

1. Purpose

In the context of Information Security, information stands for all the digital and non-digital data and assets. Information security is responsible for implementing, maintaining and improving the information security management system to keep this information secure, well-maintained in a complete form to ensure business continuity. Tasks of the Information Security Management are:

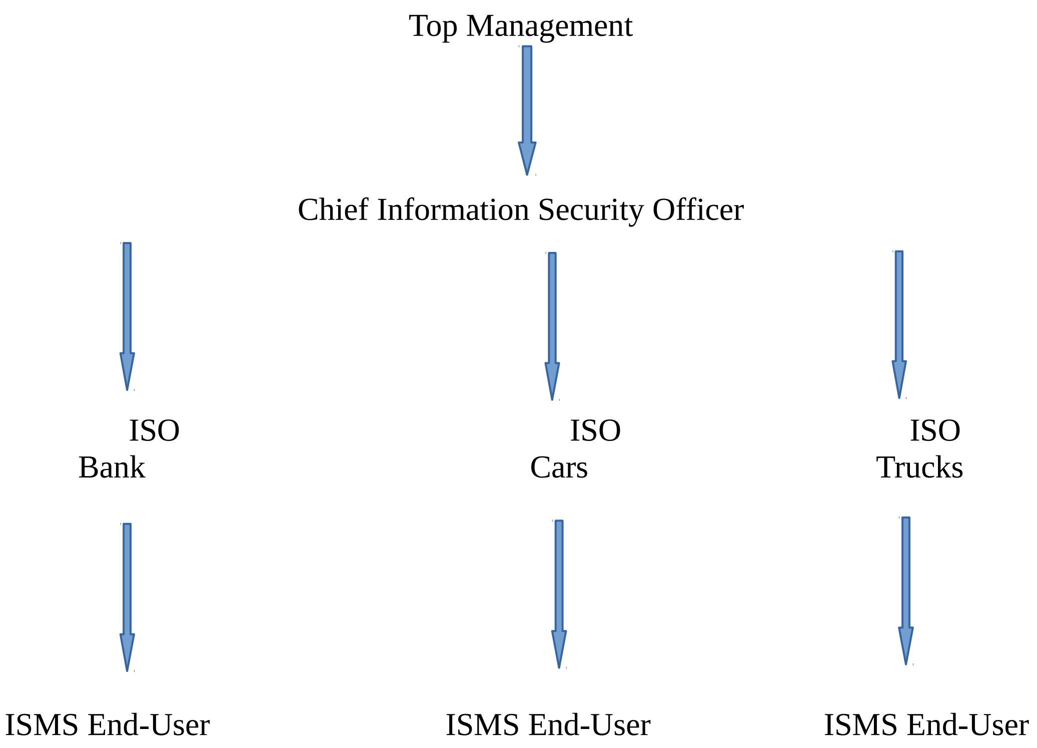
a) Definition and classification of assets according to sensitivity,
b) Definition of risks,
c) Minimization of risks,
d) Ensuring the safety of sensitive data

by accordance to business strategy, regulations, legislation and contracts.

2. ISMS Policy Reference

This general information security policy is implemented by :
-ISO 27002:2013, 5.1 Management Direction for Information Security
-ISO 27001:2013, 5.1 Leadership and Commitment
-ISO 27001:2013, 5.3 Organizational Roles, Responsibilities and Authorities
-ISO 27001:2013, A6.1.1 Information Security Roles and Responsibilities

3. ISMS Hierarchy



4. Description

OurCarComp; is an automotive manufacturer company. OurCarComp has services in the areas of banking (vehicle finance services, saving accounts and online banking); car industry (car manufacturing, development of connected cars) and truck industry (trucks according to customer needs, development of telemetrics)

4.1 Top Management

Top management should ensure;

a) information security policies and objectives are established and compatible with business strategy,
b) Integration of information security management system requirements into organization’s processes.
c) the resources for the information security management system should be available.
d) information security systems should be effective, continuous and improved.
e) the ISMS conforms to requirements and assign reporting responsibilities in addition to those listed

Top management should support information security management to other relevant management to demonstrate their leadership as it applies to their areas of responsibility.
Top management has given the authority to each team to enforce the security in their area of work.

4.2 Chief Information Security Officer (CISO) ISMS Manager

CISO is responsible of actions of information security department. Primary responsibilities for CISO are:

a) Keeping track of ISMS Vulnerabilities, organizational weaknesses and present to the management for decisions.
b) Decisions requiring implementation should be implemented with implementation team until closure.
c) Vulnerabilities for which there are no action taken should be reported to management.
d) Verification and performance of risk assessment for any new product/project/customer acquisition.
e) Controlling all documents related to ISMS.
f) Identification of new threats/vulnerabilities and reporting them to related persons.

4.3 Information Security Officer

Every ISO from different departments, is responsible of information security the department. ISOs are responsible of actions to take care of the risk according to ISMS policy and shall report to the information security management.

4.4 ISMS End-Users

a) Complies to end-user policy/procedure, namely Acceptable Usage Policy, which provides description of each user behaviour with respect to information usage.
b) Reports security weakness/incidents to either the head of department or the ISMS security manager.
c) End Users do not exploit known security weaknesses.

Abdulhay Boydedaev
Hasan Güney Esendemir
Uzezi Harry Adherioma
Araz Rustamov
Christian Bauer