Organization Standard

No.: ON.1.038

Owner:	**ZO**	Approved by:	Bohdan Wojnar	Valid from:	**03/01/2011**
Issued by:	S. Štefáček/ 19513			Note valid from:	01. 08. 2014
For EOP:	P. Opltová/17229			Replaces:	**OP 162/2**
Distribution list:	**Employee portal**				

Protective Measures

Contents:

1. Purpose

These organisation standards set forth the principles and competencies for the preparation and implementation of measures to protect Škoda Auto assets (hereinafter referred to as the company). The description of individual types of the implemented measures form a part of these organisational standards.

2. Scope of Validity

These organisation standards are valid in the company and set forth procedures for all company employees and employees of contractual partners working on company premises.

3. Basic Concepts / Abbreviations

3.1 Abbreviations

OU	Organizational Unit
IA	Intrusion Alarm
FA	Fire Alarm
CCTV	Closed Circuit TeleVision
ACS	Access Control System
MBS	Mechanical Barrier Systems

3.2 Concepts

Protection of Assets	Protection of assets rightfully in the possession of the company against, in particular, theft, damage or destruction as a result of violation or criminal offence.
Technical protection	Protection of assets using mechanical and electronic means of protection.
Building	A place, a building, a complex of buildings, a zone or a combination of these that are assessed and where protective measures are implemented.
Risk	A potential risk that assets, rightfully in the possession of the company, might be stolen, damaged or destroyed as a result of violation or criminal offence. The risk can be defined as the level of probability of the occurrence of an undesirable incident and its potential impact.

Safety Analysis	The evaluation and description of situations in terms of protecting assets, in detecting and defining risks, evaluating their importance and significance and proposals for taking relevant measures to protect assets.
Authorized Employee	A company employee authorized, in accordance with their position by the OU Manager, to deal with issues regarding the protection of persons and assets, or a third party authorized on the basis of a contract concluded with the company.
Authorized User	A company employee or a third party authorized, on the basis of a contract with the company, to operate the IA in the company.
Contractual partner	All external parties working in the company (natural or legal persons working for the company under a legally binding contract).

Effective of 1 August 2014 the following change applies:

Zone	Restricted area with a special regime of entry. The electronic system of entry checking enables only authorized MFA card holders to enter the area. Rules applying to zones are defined in Supplement 2.

Change owner: ZO

4. Competencies

Activity	Responsibility
Assessment of protection of assets, development of criminal activity and the current security situation	ZO
Providing methodical assistance in protecting assets	
Familiarizing users with the operation of technical protection devices in buildings	
Carrying out security analyses to find optimal solutions to protect company assets, including processing proposals for taking measures to eliminate risks	ZO, authorized employee
Evaluating the effectiveness of adopted measures	ZO, OU
Introducing proposed protective measures	
Complying with the given standards and procedures for implementing and the maintaining technical protection devices in buildings	
Discussing plans with the union for the introduction of protective measures involving a large number of employees	ZO, ZP, OU
Cooperation during the implementation of proposed protective measures in terms of transmitting and archiving data	ZO, EOI
Complying with rules and instructions for the operation of technical protection devices in buildings	Authorized users
Informing the ZO department about projects in preperation and requesting project security analyses	OU manager
Implementing specific measures to protect persons and assets except for measures related to the whole company the implementation costs of which are secured through separate projects	
Cooperation during the protection of assets and persons	Company employees and contractual partners

5. Procedure

5.1 Security Analysis, Determining Risks and their Assessment

The authorized ZO dept. employee, in cooperation with the authorized employee of the relevant OU, will carry out the security inspection of buildings, focusing on the actual security status of the building. Potential risks in the inspected building will be assessed along with the potential negative impacts of the risks.

5.2 Proposing Measures to Eliminate Risks

Managers of the relevant OU are informed about the content of the security analysis, i.e. with the current security status of the building in terms of protection of company assets, the established risks

and their assessment. The ZO dept. presents the managers with proposals to remove the shortcomings that had been found and together they propose a procedure for the elimination of risks and their impact.

5.3 Implementing Proposed Measures

Based on the proposed procedure to eliminate risks, the OU Manager decides how to ensure the protection of assets and implement the proposed security measures.

5.4 Evaluating Implemented Measures

After implementing proposed measures, the ZO dept. together with the relevant OU evaluate the efficiency of the proposed measures, or propose additional measures for the protection of assets.

5.5 Types of Measures, Technical Protection Devices in Buildings

Measures involving employees	include employee training, motivation, and determining responsibilities for entrusted assets.
Organization measures	include adjusting processes and procedures in order to reduce risk while protecting assets, including amending the rights and obligations of employees. These measures must not interfere with basic company activities, e.g. threaten smooth production, technical development etc.
Mechanical Barrier Systems	include means, devices and components, featuring a mechanical construction that prevents people from overcoming these obstacles (fences, gates, barriers, bars, turnstile, culverts, constructions in openings, storage buildings). The purpose of the MBS is to create a fixed barrier that is defined by its specific resistance to destruction, prevent persons entering the designated zone, damaging equipment or stealing items from the designated zone or placing dangerous items inside the designated zone.
Intrusion Alarm	is an alarm that goes off after an unauthorized entry into the designated zone at the time when the IA is activated. The IA identifies the location and time of the intrusion. The IA signal is transmitted to the central security desk. The IA is operated by authorized employees in accordance with set procedures.
CCTV	The purpose of using the systems is to detect criminal activity, to investigate incidents and events out tof the ordinary, fires and to supervise the compliance with technology regulations. The CCTV systems form a part of the preventative measures providing visual information from designated locations. CCTV systems can also be combined with other electronic security systems, such as the IA, FA and ACS. The CCTV systems are operated by authorized ZO employees. When installing CCTV, the relevant provisions of Act no. 101/2000 Sb. (on the Protection of Personal Data) and statements by the Office for the Protection of Personal Data are adhered to.
Access Control Systems (by car/on foot)	ensure that it is possible to check the persons and vehicles entering the premises, buildings and places with restricted access.
Detection Technology	includes devices for metal detection (manual and frame detectors), equipment for checking luggage, containers and vehicles (X-rays) and special detection equipment.

5.6 Planning Protective Measures

In order to ensure the cost effectiveness of protective measures, it is essential that the ZO dept. is informed in good time about any planned changes and developments in the company, in particular in terms of areal development in the company and infrastructure changes.

5.7 Implementing Protective Measures

The following must be taken into consideration while implementing protective measures:

- health and safety
- risks
- possible consequences (damage)
- value of assets that might be threatened, both material and non-material in nature
- planned changes within the development of the company, both short-term and long-term
- personnel costs and the costs of protective measures
- the development of criminal activity (on a state, regional and company level)
- anticipated results of implemented measures (purposefulness)

6. Related Documents

Act No. 40/2009 Sb. of the Criminal Code
Act No. 101/2000 Sb. on the Protection of Personal Data
Act No. 148/1998 Sb. on the Protection of Classified Information
Act No. 127/2005 Sb. on Electronic Communications
ČSN CLC/TS 50131-7 Alarm Systems – Intrusion Alarms
ČSN EN 50132-7 /334592/ Alarm Systems – CCTV systems used in security applications
ČSN P ENV 1627 Windows, doors, locks - Resistance to Forced Entry - Requirements and Classification
ON 1.004 Employee ID Cards
ON 1.022 Confidentiality
OS 122/8 Protection of Personal Data
ON.1.034 Protection of Assets
ON.1.039 Protection of Prototypes and Vehicles Subject to Confidentiality
Work Regulations
Visitor Regulations

7. Documentation

- N/A

8. Supplements

Supplement 1: Process Description: Technical Support Procedure

Effective of 1 August 2014 the following change applies:
Supplement 2: Rules applying to zones
Owner of the change: ZO

Bohdan Wojnar
Z/ Human Resources Management

Andreas Hafemann
EO/ Information systems and organization

Effective of 1 August 2014 the following change applies:

Supplement 2: Rules applying to zones

1. Categories of zones:

a) SZ/security zone
Restricted area with a special security regime (restricted and controlled access of authorized persons and security containmnet of the area) / the list of persons is available at the Employee portal.

b) KZ/Checking zone
Restricted area with registered access (limited and controlled access of authorized persons) / the list of persons is available at the Employee portal.

2. Approving a zone

A proposal to establish a zone is submitted by an OU to the ZO department. The request must contain a justification of the proposal of the security zone (incl. abbreviation) and a proposal by the zone administrator and their deputy. ZO defines the type of zone (SZ, CZ), and possibly rejects the proposal.

3. Appointing zone administrators

Administrators are appointed (and approved) by the ZO manager.

4. Entering a zone

Only an MFA card holder has the right to request access to a zone. An employee requests access to a zone in the electronic form „Establishment, change, cancellation of a zone entry permit", reg.no. 9039. A contractual partner requests zone access in the form „Request of zone entry permit", reg.no. 1559 or „Request of area T zone entry permit", reg.no. 1560. The request of zone entry permit must be approved by the respective OU manager and zone administrator for an employee and by the party requesting entry for the contractual partner (OU manager or their signing representative to whom the service is delivered by the contractual partner) and zone administrator.

Members of the Board of directors, GA manager and ZO manager are entitled to be assigned all entry permits automatically and it is in their competence to approve entry permit without the zone administrator's approval.

Deactivation of a zone entry permit is performed by ZO following a request of the zone administrator or based on a security incident.

Owner of the change: ZO