IT-Sicherheit

Inhalt:

1. Zweck
2. Wirkungsbereich
3. Grundbegriffe/Abkürzungen
4. Verantwortlichkeiten
5. Ablauf
6. Mitgeltende Unterlagen
7. Dokumentation
8. Anlagen

1. Zweck

Die Regeln zur IT-Sicherheit (Sicherheit der Informationstechnologie), die in dieser Organisationsregelung beschrieben werden, definieren die grundlegenden Ziele, die Strategie und die Verantwortlichkeiten zur Gewährleistung der IT-Sicherheit in der Gesellschaft Škoda Auto (nachfolgend Gesellschaft). Sie sind auf Grundlage der tschechischen technischen Norm ČSN ISO 27001:2005 und weiterer internationaler Vorschriften und Standards (siehe Kap. 6) definiert und sind auf deren Verankerung in der Gesellschaft ausgerichtet.
Diese Regelung knüpft an die IT-Sicherheitspolitik von VW und die mitgeltenden Vorschriften des VW-Konzerns an.
Die Gewährleistung der IT-Sicherheit umfasst die Gewährleistung der technischen Infrastruktur, die Kontrolle und Steuerung des Informationsflusses. Die Sicherheitsregeln dienen zum Schutz der Vertraulichkeit, der Integrität und der Zugänglichkeit von Informationen sowie zur Wahrung der Rechte und der Interessen der Gesellschaft und aller natürlichen und rechtlichen Personen, die mit der Gesellschaft in Geschäftsverkehr stehen oder für sie arbeiten.

Für die Schaffung und Wahrung von Vertrauen in die IT-Sicherheit werden in der Gesellschaft Vorschriften zum Informationsschutz geschaffen und realisiert, die:

- das Bewusstsein über die Möglichkeiten und Gefahren im Bereich IT, über die Gründe und die Notwendigkeit des Informationsschutzes steigern
- die IT-Sicherheit als Standard in den Prozessen der Gesellschaft einführen

2. Wirkungsbereich

Diese Organisationsregelung ist verbindlich für alle:

- OE-Leiter der Gesellschaft und die von ihnen bestimmten Mitarbeiter
- IT-Nutzer (interne und externe)
- Tochtergesellschaften

3. Grundbegriffe/Abkürzungen

IT	Informationstechnologien (sind gebildet aus IS und ICT)
IS	Informationssysteme
ICT	Informations- und Kommunikationstechnologien
Kommunikationsvorrichtungen	Personalcomputer, Arbeitsstation, Notebook, PDA (Personal Digital Assistant), MDA (Mobile Digital Assistant), Mobiltelefon
SW / Software	Satz aller Computerprogramme, die sich in der Kommunikationsvorrichtung befinden
Schädliche SW	Gefährliche SW wie Viren und andere Malware
HW / Hardware	Jedwede physisch existierende technische Ausstattung der Kommunikationsvorrichtung
Berechtigte Person	IT-Nutzer mit Berechtigung zum Lesen oder zur Änderung einer konkreten Information und des Weiteren IT-Nutzer mit Berechtigung zur Nutzung bestimmter HW
IT-Nutzer	Jede natürliche Person, die Zugang zur IT oder auf ihr gespeicherte Informationen der Gesellschaft beantragt und nutzt
Dateninhaber	Leiter der OE, wo die Daten entstehen, erstmals im IS erfasst werden, oder die die einzige OE ist, wo die gegebenen Daten verarbeitet oder genutzt werden
Information	Aktiva, die für die Gesellschaft Wert haben, können in verschiedenen Formen existieren (gedruckte, elektronische …)
Vertraulichkeit	Zugänglichmachen/Mitteilen der Information lediglich der berechtigten Person
Verfügbarkeit	Zugänglichkeit der Information für den berechtigten Nutzer im Moment ihres Bedarfs
Integrität	Gewährleistung der Wahrhaftigkeit (Richtigkeit) und Vollständigkeit der Information
Authentisierung	Überprüfung der Identifikation beim Zugang zu den Informationen
Autorisierung	Ermöglichung des Zugangs zu den Informationen nur für berechtigte Personen und nur im Umfang, der für die Erfüllung der Arbeitsaufgaben unbedingt notwendig ist
Auditierung	Erfassung und Kontrolle des Zugangs zu den Informationen
Nachweisbarkeit	Unbestreitbarkeit des Zugangs zur Information und ihrer Bearbeitung
CISO (Chief Information Security Officer)	IT-Sicherheitsbevollmächtigter – EOS Leiter, steuert die IT-Sicherheit in der Gesellschaft
ISSO (Information Systems Security Organisation)	Globale IT-Sicherheitsorganisation des Konzerns Volkswagen
Datenschutzbeauftragter	Schlägt Maßnahmen vor, die auf Erhöhung der Datensicherheit ausgerichtet sind, achtet auf einen einheitlichen Kenntnisstand in Fragen der Datensicherheit in der Gesellschaft. Auf Grundlage der Auswertung der Risiken erstellt er Datensicherheitsstandards. In Zusammenarbeit mit den übrigen OE löst er Vorfälle im Bereich der Datensicherheit.
Zuständiger Verwalter der technologischen HW	OE, in deren Verantwortung die Verwaltung der technologischen HW liegt (z. B. im Bereich V – Wartungs-OE, im Bereich T - TM/2)
EOx	Organisationseinheiten (OE), die unter EO fallen, die für die Verwaltung und die Entwicklung von IT in der Gesellschaft verantwortlich sind
ServiceDesk	Zentrale Stelle zum IT-Support der Nutzer
IT-Sicherheitsstandards	System-, Prozess- und Organisationsdokumentation, die die IT-Sicherheit betrifft
MFA2 Karte	Multifunktionsmitarbeiterausweis

4. Verantwortlichkeiten

Tätigkeit	Verantwortung
Legen gemeinsam die allgemeinen Grundsätze der Sicherheit von Informationen fest.	ZO, EOS Datenschutz-beauftragter
Macht die Mitarbeiter mit der Prozess- und Organisationsdokumentation, den Standards im Bereich der IT-Sicherheit und mit der Bedeutung ihrer Einhaltung vertraut. Ist in seinem Wirkungsbereich dafür verantwortlich, dass beim Umgang mit Informationen und IT stets eine angemessene IT-Sicherheit gewährleistet ist. Gewährleistet die Geltendmachung der IT-Sicherheitsregeln und kontrolliert fortlaufend die Einhaltung der Vorschriften. Zur Einschränkung der Sicherheitsrisiken muss er die Bildung der Mitarbeiter im Bereich der IT-Sicherheit gewährleisten.	OE-Leiter
Im Bereich der IT-Sicherheit – stellt Risiken fest, erstellt Standards und Regeln und leitet deren praktische Anwendung methodisch, führt Analysen und Audits durch, plant und kontrolliert die Durchführung effektiver Maßnahmen und löst in Zusammenarbeit mit den anderen OE IT-Sicherheitsvorfälle. Unterstützt die leitenden Mitarbeiter bei der Schaffung von Bewusstsein über die Bedeutung von IT-Sicherheit, kümmert sich um einen einheitlichen Kenntnisstand in Fragen der IT-Sicherheit in der Gesellschaft. Genehmigt Ausnahmen von den Bestimmungen dieser Organisationsregelung. Bearbeitet die Unterlagen für die Antrittsschulung der neuen Mitarbeiter der Gesellschaft (im Bereich der IT-Sicherheit)	EOS
Führt Änderungen in der HW (z. B. Installation/Entfernung von Festplatten, Diskettenmechaniken, Speichermodulen) sowie Änderungen von SW und deren Einstellung durch. Sorgt für den Anschluss der Kommunikationsvorrichtung an das Datennetz der Gesellschaft. Gewährleistet die Reparatur und Entsorgung von Kommunikationsvorrichtungen.	EOI
Führt die Verwaltung und Änderungen der technologischen HW und SW (z. B. Installation/Entfernung von Festplatten, Diskettenmechaniken, Speichermodulen) sowie Änderungen von SW und deren Einstellung durch. Gewährleistet die Reparatur und Entsorgung von technologischer HW und SW.	Zuständiger Verwalter der technologischen HW
Arbeitet mit EOS an der Schaffung von IT-Sicherheitsstandards zusammen, realisiert sie aktiv und erzwingt systemmäßig deren Einhaltung durch die Nutzer. Ist für die Gewährleistung der Sicherheitsstandards verantwortlich, plant die Beschaffung und den Betrieb von IT im Einklang mit den IT-Sicherheitsstandards. Nimmt Maßnahmen auf, damit die Zugänge zu den Informationen eindeutig identifizierbar, rekonstruierbar und unbestreitbar sind. Achtet darauf, dass lediglich eindeutig identifizierbare Personen mit der entsprechenden Berechtigung Zugang zu den Informationen erhalten können, die auf entsprechende Art geschützt sind.	EOx
Koordiniert die IT-Sicherheit im Rahmen des Konzerns VW und setzt die Einführung einheitlicher Regeln und Standards durch.	ISSO (IS Security Organisation)
Koordiniert die IT-Sicherheit im Rahmen der Gesellschaft und setzt die Einführung einheitlicher Regeln und Standards durch.	CISO (Chief Information Security Officer)

IMMER	NIE	
Ist für die ordnungsgemäße Nutzung der anvertrauten HW, SW und der Informationen ausschließlich für die Erfordernisse der Gesellschaft und im Rahmen der Erfüllung der Arbeitsaufgaben verantwortlich.	Verbreitet innerhalb der Gesellschaft und aus der Gesellschaft heraus keine Informationen mit Inhalt, der nicht die Arbeit betrifft (z. B. Kettenmails, Witze)	IT-Nutzer
Nutzt die SW und Daten im Eigentum der Gesellschaft nur auf IT der Gesellschaft.	Nutzt und speichert auf der IT der Gesellschaft keine SW, die nicht Eigentum der Gesellschaft ist, und zwar auch nicht zur Arbeitszwecken (z. B. Freeware, Shareware).	
Im Rahmen der festgelegten Aufgaben ist er für die Kennzeichnung des entsprechenden Vertraulichkeitsgrads der Informationen unmittelbar nach deren Erstellung und für ihre Sicherheit im Falle ihrer Nutzung verantwortlich.	Nutzt für seine Arbeit kein fremdes Anwenderkonto. Teilt niemandem sein Anwenderkonto und Passwort/Passwörter mit	
Geht angemessen mit den zur Verfügung gestellten IT und Informationen um, schützt sie vor Verlust, Beschädigung oder unberechtigter Nutzung oder Änderung bzw. Fälschung. Hält die Anweisungen des Herstellers und die Arbeits- und Gesundheitsschutz ein.	Nutzt zu seiner Arbeit keine private HW (inkl. Zubehör und Datenträger) und schließt sie auch nicht an die IT der Gesellschaft an (z. B. durch Anstecken eines privaten USB-Sticks an den Arbeits-PC, Anschluss eines privaten Mobiltelefons mittels Bluetooth an die Kommunikationsvorrichtung der Gesellschaft).	
Meldet seinem Vorgesetzten oder EOS/2 Störungen oder Verdacht auf Verletzung der Vorschriften betreffs der IT-Sicherheit oder Schwachstellen der IT-Sicherheit in den Systemen, einzelnen Funktionen sowie Funktionsstörungen, die für die IT-Sicherheit relevant sind.	Greift weder in die Konfiguration der HW noch in die Einstellung der SW auf den Kommunikationsvorrichtungen der Gesellschaft ein (z. B. Wechsel des RAM-Speichers, Ausschalten üblicher Dienste, Änderung der Konfiguration von IE).	
Bei der IT-Nutzung hält er die Maßnahmen zum Schutz von Vertraulichkeit, Verfügbarkeit, Integrität und Nachweisbarkeit ein.	Liefert von der zugeteilten Kommunikations-vorrichtung aus keine Daten durch Teilung an weitere Nutzer/Kommunikationsvorrichtungen, die an das Datennetz der Gesellschaft angeschlossen sind.	
Hält die Prozess- und Organisationsdokumentation und die Standards im Bereich der IT-Sicherheit ein, die ihn nachweisbar betreffen.		
Absolviert einmal jährlich eine Schulung im Bereich IT-Sicherheit.		

5. Ablauf

Die Informationen und die Anlagen, die zur Verarbeitung der Informationen und zur Kommunikation bereitgestellt werden, sind wertvolles Vermögen der Gesellschaft, das dem Schutz unterliegt. Die Übergabe von Informationen und Programmen im Eigentum der Gesellschaft an externe Organisationen (z. B. externe Personen in den gemeinsamen Projekten) ist grundlegend nur im Rahmen einer schriftlich vereinbarten Aufgabenstellung und mit schriftlicher Zustimmung des Dateninhabers zulässig.

Prinzipien der IT-Sicherheitsregeln

- Jeder, der Informationen nutzt, ist im Rahmen der festgelegten Aufgaben für deren Absicherung verantwortlich.
- Alle Informationen müssen sofort nach der Erstellung auf entsprechende Weise klassifiziert und gesichert werden.
- Nur eindeutig identifizierte Personen mit entsprechender Berechtigung können Zugang zu Informationen erhalten, die auf entsprechende Weise geschützt sind.
- Alle Zugänge zu Informationen müssen eindeutig identifizierbar, rekonstruierbar und nachweisbar sein.

Verstöße	Als Verstoß gegen die IT-Sicherheit wird absichtliches oder fahrlässiges Verhalten betrachtet, das insbesondere: • dem guten Namen der Gesellschaft schadet • die Sicherheit der Werksangehörigen, der Vertragspartner oder des Vermögens der Gesellschaft gefährdet • der Gesellschaft einen tatsächlichen oder potentiellen finanziellen Verlust verursacht • unberechtigten Zugang zu Informationen, deren unberechtigte Bereitstellung oder unberechtigte Modifikation ermöglicht • die Nutzung von Unternehmensinformationen für ungesetzliche Zwecke umfasst. Verstöße gegen die Vorschriften der IT-Sicherheit werden individuell gemäß den entsprechenden gesetzlichen, vertraglichen und betrieblichen Bestimmungen in ihrer geltenden Fassung bewertet und werden im Einklang mit den entsprechenden allgemein verbindlichen Rechtsvorschriften sanktioniert.
Anschluss von Kommunikations-vorrichtungen ans Datennetz der Gesellschaft	Der Anschluss einer Kommunikationsvorrichtung ans Datennetz der Gesellschaft ist nur dann gestattet, wenn sich die Vorrichtung im Eigentum der Gesellschaft oder einer solchen Gesellschaft befindet, in der die Gesellschaft Škoda Auto oder eine der Gesellschaften des Volkswagenkonzerns einen Mehrheitsanteil hat. Der Anschluss darf nur von EOI vorgenommen/eingestellt werden.
Sicherung der IT gegen Verlust, Beschädigung und Diebstahl	Mit der IT der Gesellschaft muss angemessen umgegangen werden und sie muss vor Verlust, Beschädigung oder Diebstahl geschützt werden. Die Kommunikationsvorrichtung darf nicht ohne Aufsicht frei zugänglich bleiben. • Der Transport von Kommunikationsgeräten über die Grenze der Gesellschaft hinaus ist nur mit schriftlicher Zustimmung von ZO möglich (mit Ausnahme der Mobiltelefone). • Tragbare Kommunikationsvorrichtungen dürfen nicht unbeaufsichtigt im Kraftfahrzeug aufbewahrt werden. • Bei Reisen mit dem Flugzeug und dem Zug muss die tragbare Kommunikationsvorrichtung grundlegend als Handgepäck transportiert werden.
Sicherung der IT vor unberechtigter Nutzung	Zu den Kommunikationsvorrichtungen der Gesellschaft dürfen nur berechtigte Personen Zugang haben. Unberechtigte Personen (gilt auch für Familienmitglieder, Freunde usw.) dürfen keine Möglichkeit haben, das Gerät zu benutzen oder Einsicht in Informationen zu bekommen, die mit dem Level intern, vertraulich oder geheim klassifiziert sind (siehe ORL – 161/3 - Geheimhaltung). Falls auf der Kommunikationsvorrichtung eine lang andauernde Bearbeitung gestartet wurde, die nicht unterbrochen werden kann, oder wenn der Nutzer sich für eine bestimmte Zeit unbedingt vom Gerät entfernen muss (z. B. Pause, Verhandlung, Toilette), muss der Nutzer die Kommunikationsvorrichtung durch einen passwortgeschützten Bildschirmschoner oder einen ähnlich funktionierenden Mechanismus gegen unberechtigte Nutzung absichern. Nutzer, die zur Anmeldung ins System eine MFA2 Karte benutzen, müssen bei jedem physischen Entfernen von der Kommunikationsvorrichtung die MFA2 Karte aus dem Lesegerät herausnehmen. Nach Beendigung der Arbeit mit der Kommunikationsvorrichtung ist der Nutzer verpflichtet, eine ordnungsgemäße Beendigung des Systems vorzunehmen und das Gerät, einschließlich des Monitors sowie aller direkt angeschlossenen Kommunikationsgeräte, auszuschalten.

Sicherung der Endgeräte vor schädlichen Programmen (Antivirenprogramm und Sicherheitsaktualisierungen der SW)	Die Regeln zum Schutz vor Viren und schädlichen Programmen legt die MA Virenschutz fest. Die Kommunikationsgeräte, Systeme und Datenträger müssen regelmäßig und bei Verdacht auf das Vorkommen einer schädlichen SW sofort mit Hilfe einer aktualisierten Antiviren-SW kontrolliert werden (wird auf Büro-PC durch das Virenschutzprogramm automatisch gewährleistet). Bei Verdacht auf Befall von einer schädlichen SW oder Funktionsunfähigkeit des Virenschutzprogramms darf die Kommunikationsvorrichtung nicht weiter genutzt werden, und der ServiceDesk (bzw. der zuständiger Verwalter der technologischen HW) muss informiert werden, der die Entfernung der schädlichen SW gewährleistet. Sicherheitsaktualisierungen werden auf Büro-PC automatisch installiert und der Nutzer wird über deren Installation informiert.
Sicherheit der elektronischen Post/des Internets	Die elektronische Post muss automatisch auf das Vorhandensein unerwünschter Nachrichten (sog. Spam) überprüft werden. Diese unerwünschte Post muss automatisch gelöscht werden. Sollte der Nutzer trotzdem in seinem Posteingang unerwünschte Post finden, sollte er diese löschen, ohne sie zu öffnen. Das Erstellen, Absenden und Weiterleiten von unerwünschten geschäftlichen oder privaten Ketten- und Massenmitteilungen ist verboten. Die elektronische Post ist nicht zur Übergabe großer Dateien bestimmt. Der Absender ist als Urheber der elektronischen Nachricht für den Inhalt und den Verteiler verantwortlich, der Empfänger ist für die Weiterbearbeitung und Verteilung der elektronischen Nachricht verantwortlich. Elektronische Nachrichten und ihre Anlagen müssen vor dem ersten Starten durch eine aktuelle Virenschutzsoftware auf das Vorkommen gefährlicher Software kontrolliert werden (wird auf Büro-PC durch das Virenschutzprogramm automatisch gewährleistet). Das Internet darf nur zu Arbeitszwecken genutzt werden. Nähere Spezifikationen und Nutzungsregeln siehe OA 123/2 – Internet – Zugriffsberechtigung und Betrieb.
Sicherheitskopien	Informationen dürfen ausschließlich nur auf den dafür bestimmten Netzlaufwerken gespeichert werden, wo deren zentrale und automatische Sicherheitskopie sichergestellt wird. Das Speichern von Informationen auf der lokalen Festplatte der Kommunikationsvorrichtung ist nur für vorübergehenden Arbeitsbedarf möglich. Speicherplatz auf nicht technologischen PC mit dem Betriebssystem Windows darf einzig und allein der Ordner Dokumente (sog. Anwenderprofil des gegebenen Nutzers) oder seine Unterordner sein. Der Nutzer ist für die Sicherheitskopien der Daten, die auf lokalen Datenträgern gespeichert sind (Festplatten der Kommunikationsvorrichtungen, CD, DVD und weitere) und deren eventuellen Verlust verantwortlich. Datenträger, die vertrauliche oder geheime Daten beinhalten, müssen auf entsprechende Art gekennzeichnet, katalogisiert und in verschlossenem Raum (Schrank, Schublade) aufbewahrt werden.
Zugang des Nutzers zu Informationen	(Außer zu öffentlichen Informationen) darf der Nutzer nur zu den Informationen Zugang erhalten, die er im Rahmen der Erfüllung seiner Arbeitsaufgabe benötigt. Einen größeren Umfang muss der Dateninhaber nachweisbar genehmigen. Ein Anwenderkonto oder eine Zugangsberechtigung, die nicht mehr benötigt werden, muss der Nutzer dem zuständigen Errichter des Zugriffs melden, der zu dessen Löschen verpflichtet ist. Unbenötigte Identifikationsmedien (z. B. MFA2 Karten, SecureID tokens) müssen unverzüglich dem Herausgeber oder der beauftragten OE

zurückgegeben werden.

Den Zugang zu Informationen, die Arbeit mit ihnen und ihre Speicherung auf den Netzlaufwerken regelt die MA EOI Arbeit mit Daten im Netz.

Erfassung der Kommunikations-vorrichtungen	Jede Kommunikationsvorrichtung im Eigentum oder in der Nutzung der Gesellschaft muss in der zentralen IT-Erfassung erfasst werden. (Näheres siehe MA IT-Erfassung).

6. Mitgeltende Unterlagen

Gesetz Nr.140/1961 GBL Strafgesetz
Gesetz Nr.101/2000 GBL Gesetz über den Schutz persönlicher Daten
Gesetz Nr.148/1998 GBL Gesetz über den Schutz vertraulicher Fakten
ČSN ISO/IEC 27001:2005
ISO/IEC 9001:2000
Sicherheitspolitik IS VW und mitgeltende Vorschriften des VW-Konzerns
Politik der Gesellschaft Škoda Auto
Handbuch des integrierten Managementsystems Škoda Auto
ORL 122/4 Datenschutz und Datensicherung
ON.1.019 Zugriffsberechtigungen in Informationssystemen
OA 123/2 Internet – Zugriffsberechtigung und Betrieb
ORL 161/3 Geheimhaltung
ORL 162/2 Schutzmaßnahmen
ORL 162/3 Vermögensschutz
Arbeitsordnung
Intranet EO:
- MA Arbeit mit Daten im Netz
- MA Virenschutz
- MA IT-Erfassung

Intranet EOS:
- Anwenderkonto und Zugang des Nutzers zu Informationen – Festlegung von Passwörtern und PIN

7. Dokumentation

Formular Berechtigung zur Mitnahme der Gegenstände aus dem Werksareal heraus

8. Anlagen

Nicht besetzt

Holger Kintscher
E/Kaufmännischer Bereich

Andreas Hafemann
EO/Informationssysteme und Organisation