VOLKSWAGEN FINANCIAL SERVICES

FINANCIAMENTOS. CONSÓRCIO. SEGUROS. MOBILIDADE.

Our Information Security Policy – Abbreviated Version

1. Introduction

This "Information Security Policy" (hereafter "IS Policy") is a strategic document describing the handling of information security within Volkswagen Financial Services Brazil (VWFS).

It is the binding commitment of high-level management, aiming to achieve a level of Information Security throughout the VWFS. This heightens the importance of information as an essential business asset that needs protection for the benefit of all VWFS' employees (internals, students and externals that execute any sort of activity for VWFS) and customers.

Responsible management and the information protection ensure the security of company assets and the continued provision of financial services by VWFS as a company.

The activities resulted from the information security policy are part of the strategy and support the achievement of the compliance and governance goals.

This document represent the highlights of the main topics from the VWFS IS Policy. The full version of this Policy and its related documents are available for all employees and third parties of Volkswagen Financial Services Brasil.

2. Description

2.1. Goals

Preserve and protect the VWFS information, or any other information that are under its responsibility, as well as, IT resources that protect them from the many sort of threats, and support them during their lifecycle, no matter the mean or the format.

Information protection is based on the basic information security values mentioned below (the so-called protection objectives), which are components of all operational actions and therefore need to be considered at all times. They are:

• **Confidentiality:** Information or functions should only be available to groups of people with the relevant permissions.
• **Integrity:** The integrity of the information must be safeguarded at all times. The information must be correct and complete. Functions should provide correct results.
• **Availability:** For those, which the use of the information and functions is allowed, the access shall be always possible, within the required timeframe and with the necessary level of quality.
• **Authenticity:** The authenticity shall be provided from an authentic, reliable and responsible source. It should be ensured that it did not mutate throughout the process.

The objective is to guarantee the level of protection defined for the respective business processes as well as for the processed information via appropriate measures on organizational as well as technical levels (security level).

Furthermore, this policy aims to stablish the responsibilities and limits the practice of VWFS employees and customers in regards to the information security and communication, reinforcing the internal culture and prioritizing the required actions due to the asset criticality.

These measures aim to enable the VWFS to prevent, detect and reduce vulnerability to information-related incidents in either the standard technology (data center, internal systems) or

cyber environment (using the internet as a resource) – as well as in the physical environment (physical documents, information stored in safes, etc.).

Information sharing initiatives along with other financial institutions about relevant information security incidents are also encouraged.

2.2. Principles

In order to be able to protect information efficiently and goal-oriented, the following principles form the basis for VWFS security strategy:

- **Prevention**
- **Reaction**
- **Sustainability**

Awareness, training and education measures for the handling of information technology, as well as processed information protection, are mandatory to maintain the information security baselines. Those measures cover not only our employees, but also our vendors and clients – this webpage is a live example of this.

The above principles are embodied through comprehensive information security policies and guidelines. Its implementation can be supported through specific work instructions and standard operating procedures.

2.3. Information Security Process

VWFS operates in accordance with the ISO/IEC 27001:2013 standard and it has implemented its corresponding Information Security Management System (ISMS).

Based on this, the general requirements for the ISMS are defined; the roles, responsibilities and documentation requirements are specified; internal ISMS reviews are performed; and this framework is continually improved through corrective and preventive measures. If ISO/IEC 27001:2013 specifications are not sufficient for processes, other recognized frameworks can be used in Information Security management (e.g.: NIST, COBIT, etc.).

All stakeholders ensure achieving protection goals and adhering to information security principles at VWFS through a joint approach as part of a continuous information security process.

The policies, guidelines, process manuals, and role descriptions that are required for this are provided in individual documents.

2.3.1. Procedures, Controls and Monitoring

Procedures and monitoring activities are in place to reduce VWFS vulnerability to security incidents, and to address other information security objectives.

These controls include processes that support information tracking and the enhanced security of confidential and sensitive information.

All of these controls are applied to the development of secure information systems and the adoption of new technologies employed in VWFS activities. They observe the levels of complexity, comprehensiveness, and accuracy that are consistent with those used by VWFS and the risk appetite defined by the VWFS governing body.

Regarding relations with service providers and resident third parties, procedures and controls should be implemented to prevent and manage incidents to be adopted by them, especially those handling sensitive data or information or relevant to the conduct of the VWFS operational activities.

Another important method for information control is the Information Classification Process. It guides VWFS team on the information categorization, and determines protective measures based on such classification (Public, Internal, Confidential and Secret).

2.4. Intellectual Property

Every data record, voice or image storage on magnetic, optic or electronic means from VWFS or yet other graphic or paper reports or even other exhibition means, comprise company's information property or information under its responsibility, where every component from the computing environment must have an information owner.

The information owner shall ensure that all components from the system or service are available and that they attend information security requirements, especially the ones regarding information classification, labelling and discard.

2.5. Personal Data Protection

VWFS has the commitment to promote the compliance to the privacy and financial protection laws of its customers' data. It has to ensure availability, integrity, confidentiality and the authenticity of personal data, during all its lifecycle, considering any method of storage or support, through:

• Personal data processing in compliance to the current data protection regulations;
• Adoption of security measures to protect the personal data from non-authorized accesses, accidental or illegal destruction, loss, change, inappropriate or unlawful communication or processing;
• A safe, controlled and protected storage;
• Application of anonymization and pseudo anonymization procedures, whenever is needed and possible;
• Application of encryption protocol when transmitting and storing data, whenever is needed;
• Record personal data processing operations;
• Safe discard of personal data by the end of its purpose and its safeguard in accordance to the legal and regulatory pre-approved custody situations;
• Transfer data to third parties on safe ways as contractually agreed;
• Impact and systematic assessment to privacy and data owners;
• Appropriated management and handling of incidents that involve personal data;
• Regular execution of tests, monitoring and assessment about the effectiveness of these measures.

2.6. Business Continuity Planning

Contingency planning shall be documented for all business operations and it shall include an assessment of critical impacts to business operations, definition of procedures that facilitate continuity of work in emergencies, critical systems' continuity planning and procedures for reestablishing operations.

Business Continuity tests should be performed on a regular basis, based on disasters and security incident scenarios in order to ensure that teams are prepared in the event of such situations.

2.7. Violations and infringements handling

Failure to comply with the rules will subject the infringer and those who collaborate with him, to the penalties described in the VWFS disciplinary proceedings and/or in the contracts by which the resident third parties and/or service providers are signees.

Violations include deliberately and grossly negligent activities, in particular those that:

- Compromise the information security of the VWFS employees and contractual partners;
- Damage VWFS reputation;
- Cause the company to suffer actual or possible financial damage;
- Allow unauthorized access to information or the distribution and/or change of this information;
- Result in a violation of the right to determine how information is used (data protection violations);
- Constitute violations of laws, regulations or contracts;
- Prevent completion of tasks (e.g. with regard to efficiency and capacity); or
- Allow the use of VWFS information for illegal purposes.

Any non-compliance with information security regulations should be reported and forwarded to the IT Governance - Information Security area through the e-mail address: **seginfo.brasil@vwfs.com**.

2.8. Roles and responsibilities

The secure operation of business processes in VWFS, along with the information technology necessary for this; require roles and responsibilities to be clearly defined. The tasks, competencies and responsibilities of the respective roles within the ISMS are described in individual documents.

Questions in regards to this document shall be forwarded to our customer service channels.