VOLKSWAGEN FINANCIAL SERVICES

FINANCIAMENTOS. CONSÓRCIO. SEGUROS. MOBILIDADE.

Information Security Guidelines for Vendors

1. Objective

This document aims to establish the guidelines, principles and responsibilities as well as guide the implementation of actions related to information handling and the appropriate use of assets by suppliers, partners and business stakeholders of the VWFS.

2. Scope

The contents of this appendix apply to all suppliers, partners and stakeholders of VWFS.

3. Responsibilities

It is the responsibility of suppliers, as well as their respective employees assigned to provide services to the companies of the Volkswagen Financial Conglomerate, to ensure the protection of information assets in order to achieve the following objectives:

Confidentiality: ensuring that the information processed is exclusively known to specifically authorized persons;

Integrity: ensuring that information is kept intact without undue modification – accidental or intentional;

Availability: ensuring that information is available to all persons authorized to handle it.

Compliance: Comply with the processes that guarantee the rights and obligations provided for in the contract, as well as aspects of audits and regulations, within the ethical principles and conduct established in the VWFS Code of Conduct and Ethics - Suppliers.

4. 4. Information Security definitions

4.1. What is Information Security?

Information is an asset of VWFS. Information that is collected, used, stored and eventually transmitted by VWFS is essential for the daily work of its areas.

Information security is a set of actions and controls to protect information, software and IT infrastructure from problems related to the safe disclosure, change, suspension and disposal of information. Information Security requirements for confidentiality, integrity, availability and compliance should be practiced in all respects as a priority in physical or digital means.

In view of the growing need to maintain a protected environment, we emphasize that an effective awareness program is essential for all VWFS suppliers, partners and stakeholders.

4.2. What kind of information to protect

Those who have access to VWFS systems and/or access company information need to protect information according to their classification:

Secret Information: Information that may threaten the achievement of company objectives in a sustainable manner if it is obtained by unauthorized persons. They should therefore be the subject of an extremely restrictive and tightly controlled distribution list.

Confidential Information: Information that may threaten the implementation of a product and or project objectives if it is obtained by unauthorized persons. They should therefore be made available to a limited circle of authorized persons. This category also includes personal data that in context allows natural conclusions to be drawn about a person.

Internal Information: Information that is not intended for public disclosure and should only be disclosed to the VWFS. Those information shall not be distributed to third parties, unless:

- Such information is categorized as public;
- The owner approved the distribution of the information; or
- External parties depend on information for cooperation purposes.

4.3. Protection Needs Analysis - PNA

A component of the Risk Management Platform, the Protection Needs Analysis process has been defined and implemented by the VWFS to identify and mitigate mapped risks. The purpose is to define an appropriate level of protection for company systems, as well as providing visibility into the business areas' dependence on IT systems/services and structure, including the participation of vendors related to those services/products.

The protection need analysis defines which protection measures are appropriate and relevant to:

- the business processes;
- the information processed there; and
- the used information technology.

Defined Protection Needs for the company's information assets form an important basis for managing operational risks related to information security and information technology.

Based on the protection goals for business processes, called information security pillars, namely:

- Confidentiality;
- Integrity;
- Availability; and
- Authenticity.

In case the supplier, partner or stakeholder is classified as critical because of this analysis, a contract amendment shall be signed describing the protection measures that shall be applied in the managed environment.

4.4. Minimum Requirements

All suppliers, partners and stakeholders of VWFS companies must follow the information security governance and controls requirements listed below:

- Have an updated Information Security Policy and ensure its employees know about it;
- Maintain a security incident management process;
- Maintain a safe and healthy environment by using malware tools;
- Use of compatible encryption resources, when applicable;
- Follow the deadlines and response time provided for in the contract;
- Train its employees on good practices for information security and personal data protection;
- Keep records of the performed personal data treatment operations;
- Provide the communicate channels of the company's Data Protection Officer or the internal staff with the same attributions.

Evaluations of the services provided are periodically made, as well as checks on the application or practice of the requirements described in items 4.3 (Protection Needs Analysis) and 4.4 (Minimum Requirements) described above. Failure to comply with or deviate from any of the above requirements may result in disciplinary actions and application of legal or contractual sanctions.

4.5. Information Security Responsibilities

Each outsourced employee must ensure that security rules are respected when dealing with VWFS information or information processing systems with the following practices:

- Know and comply with the guidelines set forth in this document and other related Regulations;
- Prevent unauthorized access and Social Engineering;
- Watch out for and guard against malicious code or Malware, Spam, Phishing and Social Engineering actions;
- Implement security measures, technical and administrative, aiming to protect non-authorized accesses to information as well as risk situations or unappropriated or illegal treatment;
- Immediately inform VWFS Information Security team about risk situations that may compromise the company's data, information and image;
- Do not share credentials (ID, passwords and badge);
- Participate in training offered by the Information Security area of the VWFS on this topic;
- Maintain best practices recommended by the VWFS Information Security area.

Any violation of safety rules may result in disciplinary measures and sanctions provided for by law and in the contract signed with the VWFS.

4.6. Personal Data processing

4.6.1. Processing

Suppliers, partners or stakeholders that process personal data or sensitive personal data ("confidential information") that are under the VWFS control, shall follow the processing instructions provided.

The supplier, partner or stakeholder shall request previous authorization to VWFS in case they identify a need to process personal data in a different way than the provided instructions.

The personal data processing related to services handled with further parties, especially the transmission and processing, excepting the transmissions occurred in the force of the law, shall occur only after a previous and formal authorization of VWFS.

4.6.2. Sub processors

The supplier, partner or stakeholder may subcontract part of the services that involve personal data processing to one or more parties (“sub processors”) due to a pervious and formal authorization from VWFS.

When authorized, the supplier, partner or stakeholder shall sign a written contract with the sub processor formalizing the same criteria, technical and organizational measures and VWFS instructions.

4.6.3. Monitoring

VWFS may verify the fulfilment of the presented instructions as well as the further regulation that are related to personal data.

The supplier, partner or stakeholder shall monitor, through adequate means, its own compliance and authorized sub processors’, against the personal data protection instructions and shall provide to VWFS reports about these controls whenever requested.

The reports abovementioned shall include, at least: (i) status of the personal data processing systems; (ii) applied security measures; (iii) recorded inactivity time of the security technical measures; (iv) the stablished (non) compliance with the organizational measures; (v) any eventual data violations and/or information security incidents; (vi) the noticed threats to the security and to the personal data; and (vii) the demanded and/or recommended improvements.

Every time VWFS request such reports, they shall be provided until 48 (forty-eight) hours.

4.6.4. Rights exercising

The supplier, partner or stakeholder shall notify until 24 (twenty-four) hours the VWFS Information Security team, which is described on item 4.14 of this document – “Information Security”, about eventual requests of personal data owners which are under the VWFS control. E.g. personal data confirmation of existence; correction of incomplete, incorrect or outdated data; among other rights stablished by law.

The supplier, partner or stakeholder shall provide mechanisms so VWFS can execute the required actions to attend the personal data owners requisitions under its control, especially: (i) confirm the existence of personal data of such owner; (ii) have access to the personal data from such owner; (iii) correct or request the correction of incomplete, incorrect or outdated personal data; and (iv) request the processing discontinuation or the discard of personal data of such owner.

4.6.5. Data processing record

The supplier, partner or stakeholder shall record the processing activities executed in the personal data under the control of VWFS, including: (i) record of the user that performed such processing; (ii) the type of processing; (iii) the date and time of processing; and when applicable (iv) the sub processors with date and time of the transmission and or type of processing and (v) further controllers, with date and time of the data distribution.

4.6.6. New products or services

Except due a counter commercial condition expressed in the contract, the supplier, partner or stakeholder shall not transmit, share or sale any information, product or service created from the processing of personal data under the control of VWFS.

4.6.7. International Transfer

In case the supplier, partner or stakeholder has the intention to make transfer and/or processing of the personal data under the VWFS control outside of Brazil, it should request previous and formal authorization to VWFS.

4.6.8. Notification

The supplier, partner or stakeholder shall notify within 24 (twenty-four) hours the VWFS Information Security team about: (i) any violation (even suspicious) of the legal requirements concerning Personal Data Protection; (ii) any noncompliance to the agreed obligations concerning personal data processing; (iii) any security violation from its sub processors; (iv) any exposition or threats related to the Personal Data protection compliance; (v) or, in small period, if necessary, any order from Courtroom, public authority or regulatory agency.

4.6.9. Personal Data protection impact report

Whenever required, the supplier, partner or stakeholder shall provide clear information about personal data processing processes and the related applied measures and mechanisms so VWFS can issue or keep updated the Personal Data protection impact report.

4.6.10. Discard

After the fulfilment of the processing purpose and upon the end of the contractual agreement, the supplier, partner or stakeholder shall return and/or eliminate the personal data under the VWFS control, processed on a safe mode, independently of their state (physical or digital).

The exception for the non-elimination of a personal data is only when its safeguard is associated to the fulfillment of a legal obligation. Shall exception shall be formalized to VWFS with the retention period information of such data and the applied security controls.

4.7. Use of Company Network

Only company-owned computers are allowed to be used on the VWFS' corporate network. WLAN guest networks are an exception to this rule; however, requests for such access should be logged through service requests to the IT Operations Team and authorized by the VWFS Information Security team.

4.8. Transmitting data and programs

Data and software may only be transmitted to outside corporations, authorities, institutions and other third parties outside the VWFS if allowed and complying with existing regulations, instructions or procedures. They shall specify that the "electronic" transfer of messages, texts, tables and graphics be allowed to be sent only after confirming the existence of such written and signed rules between the parties.

The transfer of software data to outsiders contractually linked to the VWFS (e.g. members of remotely allocated project teams, etc.) is permitted under this task when agreed in writing.

Transmission of data from within the network for exchange with external companies should be handled based on written orders or contracts.

Transmission of personal data or sensitive personal data shall occur only via channels that allow the application of security controls and using encryption methods.

For physical transportation, data envelopes must be labeled in accordance with Corporate Security instructions indicating the order of transportation.

4.9. Document Encryption

Secret information should only be stored and transmitted encrypted.

The exchange of non-public information with external parties via email or similar communication channels should be encrypted. State-of-the-art encryption algorithms should be used.

The encryption capability of compression tools should be used to encrypt non-public email information for all other companies or in cases where the headquarters email system does not use a second authentication factor (PKI). In this case, the password used must be communicated via a different communication path (e.g. telephone), and used only once.

4.10. Return of VWFS assets

Upon termination of the contract, the outsourced employee must return all assets owned by the VWFS, including equipment, records and notes.

4.11. Relevant Processing, Data Storage, and Cloud Computing Contracts

Suppliers contracted to provide the abovementioned services must meet the following requirements:

a) Ensure VWFS a no limited access to the data and information to be processed or stored by the service provider;
b) Ensure the confidentiality, integrity, availability and recovery of the data and information processed or stored by the service provider;
c) Provide evidences as to their adherence to certifications required by VWFS to provide the service to be hired;
d) Provide VWFS access to reports prepared by an independent specialized audit firm hired by the service provider, relating to the procedures and controls used to provide the services to be contracted;
e) Provide appropriate management information and resources for monitoring the services to be provided;
f) Identify and segregate customer data from the VWFS through physical or logical controls;
g) Ensure the quality of access controls aimed at protecting VWFS data and customer information;
h) In the case of running applications over the internet, the service provider shall adopt controls that mitigate the effects of potential vulnerabilities when releasing new versions of the application;
i) Contracts must include the following items:

i. Indication of the countries and region in each country where services may be provided and data may be stored, processed and managed;
ii. The adoption of security measures for the transmission and storage of the data mentioned in item i;
iii. Maintaining, as long as the contract is in effect, data segregation and access controls to protect customer information;
iv. The obligation, if the contract is terminated, to:
- Transfer of the data mentioned in item I to the new service provider or contracting institution; and
- Deletion of the data mentioned in item I by the replaced contractor after the data transfer provided for in sub-paragraph "a" and confirmation of the integrity and availability of the data received;

v. The contracting institution's access to:
- Information provided by the contractor to verify compliance with the provisions of items I to III;
- Information regarding certifications and specialized audit reports, mentioned in items “c” and “d”; and
- Appropriate management information and resources for monitoring the services to be provided, mentioned in item “e”;

vi. The contract in question must provide, in case of decree of resolution regime of the contracting institution by the Central Bank of Brazil;
- The obligation on the contractor to grant full and unrestricted access by the person responsible for the settlement to contracts, agreements, documentation and information relating to the services provided; stored data and information about its processing, backups of data and information, as well as access codes, mentioned in item “iii”, which are held by the contracted company; and
- The obligation to give notice to the person responsible for the resolution scheme the intention of the contractor to discontinue the provision of services at least 30 days prior to the scheduled interruption date, provided that:
  - The contractor undertakes to accept any request for an additional thirty days for interruption of service, made by the person responsible for the resolution regime; and
  - Prior notification shall also occur in the situation where the interruption is motivated by the VWFS' default.

The definition of the service relevance is made by the VWFS, and may be changed over the contracting period if there are changes in the type of information stored or processed by the service. The VWFS will be responsible for informing the supplier of its business relevance, including the need for related contractual changes.

4.12 Information Security Incident

The VWFS has a comprehensive Information Security Management Process for handling Information Security incidents.

An information security incident may threaten the privacy or security of information. They may be accidental or intentional, including theft, loss, unauthorized change or destruction of information. An information security incident is considered when, especially, a privacy violation is identified.

A critical incident should be considered when the compromised data includes personal information such as name, date of birth, health, financial and confidential information.

Truth and cooperation are vital to the information security incident management process. The key to responding appropriately to an incident is to take appropriate action as soon as possible. The following recommendations should be followed in case or suspected of an incident:

(i) Inform

• Immediately report irregularities to the VWFS Information Security team;
• Describe the situation exactly as it occurred to avoid further damage;
• If possible, on first contact provide an estimation of damage size, consequence of damage, affected parts (internal, external) and possible consequences.

(ii) Implement measures

- Follow instructions from information security team and IT administrators of VWFS;
- Only take additional measures if advised by authorized persons;
- Do not provide any information to uninvolved persons without explicit authorization;
- Communicate VWFS Information Security team about the progress of the plan and the implementation status of the measures.

Suppliers and partners that handle sensitive data or relevant information to conduct VWFS operations, should promptly report to the given channels the event of Information Security Incidents in their environment that in any way affects VWFS.
The suppliers, partners or stakeholders shall cooperate with VWFS by providing the available relevant information and any further assistance to document and eliminate any security violation cause and imposed risks.
All procedures executed during an incident handling shall be documented by the involved parties, under the supervision of the VWFS Information Security team.

4.13 4.13 Continuity plan for the technology services

The suppliers, partners or stakeholders shall ensure the continuity of the provided services within the defined service level agreements.

The providers classified as critical by VWFS, concerning IT services continuity, take a key role within this context. They have the responsibility to perform regular technical or operational contingency tests (depending of the hired service), in order to verify its capacity to attend to the defined service level agreements, and shall present the related evidences on annual basis.

4.14. 4.14 Who to Contact in Information Security

Problem / Incident	Contact
• Relevant Events • Suspicion/evidence of an information security incident (e.g. virus infection) • Loss/theft of company information or equipment • Data Privacy issues • General IT security issues	Local Information Security Officers seginfo.brasil@vwfs.com