VOLKSWAGEN

GROUP OF AMERICA

IT-04: Data Usage and Governance

Effective Date	July, 2018 (v5)
Responsible Department	IT&S Information Security
References	Regulation 02.02
Data Classification	Internal

Table of Contents

1. Purpose 1
2. Data Security & Transmission 1
3. Data Usage & Sharing 2
4. Violations 3
5. Signatures 4

1. Purpose

Volkswagen Group of America, Inc. and all its direct and indirect subsidiaries and organizational units (collectively, the "Company") establish this policy to address every Employee's and Vendor's responsibilities regarding the use, sharing and transmission of Company data. This policy applies to the Company including all employees, contractors, and third-parties performing activities on behalf of the Company.

2. Data Security & Transmission

The Company views all data which is available from any system within the Company computer environment OR on any system outside of the Company environment that contains Company specific information as private. The transmission of data classified as Internal, Confidential or Secret (reference IT-12) falls under strict guidelines.

Data transfer requests with 3rd Parties must be submitted via the internal IT Services (e.g. iServe) portal and must obtain appropriate approvals and/or ensure non-disclosures agreements are in place prior to any data exchange.

Examples of transfer methods are as follows:

- Examples of approved transfer methods for "**Internal**" data include SFT, Corporate Box, Secure (TLS) Corporate Email.
- Examples of approved transfer methods for "**Confidential**" data include Secure Data Exchange (SDX), Encrypted Email (PKI), Confidential (Totemo) Email, with Security approval encrypted/password protected files via Box and SFT.
- Examples of approved transfer methods for "**Secret**" data include SDX, Encrypted Email (PKI).
- Any exceptions must be approved by the IT&S Information Security.

3. Data Usage & Sharing

Vendor usage of data

The Company has many Vendors which perform valuable services using data provided by the Company. To protect itself from legal liability and loss of governance and knowledge of data usage, any Vendor doing data related business with the Company is contractually subject to the following rules related to data usage. Any Employee of the Company who engages a Vendor to perform data-related services is required to enforce these rules as described below.

- Vendor must ensure that data will be handled in a secure manner taking every precaution to prevent the data from being shared, manipulated or stolen
- Vendor must use one of the data transfer mechanisms based on the data classification and requirements from Enterprise Data Management team.
- Vendor must provide transparency as to the architecture which will be used to secure the data once in the Vendor's possession.
- Vendor will not attempt to re-sell unaltered data back to the Company without the written consent.
- Vendor will not attempt to sell or transmit Company data to any other vendor without the written consent.

IT-04: Data Usage and Governance

- Vendor will fully disclose any and all intended usage of or enhancements to the data being provided.
- Current Non Disclosure Agreements (NDAs) need to be in place and on file at all times while doing business with the Vendor.
- Current Vendor Data Usage Agreement (VDUA) needs to be in place and on file at all times while doing business with the Vendor.

Usage of Data

Access to data will be restricted to the level of detail required to meet their business needs. Access to and usage of the data will be audited periodically. Employees who are granted access to detailed level data are expected to treat the data as private and confidential and are subject to the following guidelines.

- Detailed data cannot be shared outside of the Company. If a need exists, permission must be granted from the IT&S Information Security team and a NDA and VDUA must be signed by the party receiving the data. Ideally, if a recurring need to exchange data exists, a scheduled process should be created to perform this activity.
- Analysis/rollup/aggregated information can be shared provided the party the data is being shared with has a NDA and VDUA on file with the Company. It is the Employee's responsibility to verify that a NDA and VDUA is on file prior to sharing any data outside of the Company. Verification of NDA and VDUA can be done by emailing the IT&S Information Security team (InfoSec@vw.com). If a NDA and/or VDUA is not on file a Service Request must be submitted.
- Any Employee aware of unauthorized data usage or sharing should report the violation to the IT&S Information Security team (InfoSec@vw.com).

4. Violations

Violations of this policy may subject the person responsible to disciplinary action up to and including termination of employment. Further, an Employee's obligations as provided herein will survive the Employee's departure from the Company for any reason, including separation, termination and retirement. Such obligations will not be affected by any severance agreement or

similar document entered into at the conclusion of employment. Violations of this policy by any Vendor doing business with the Company may result in the loss of the contract to do business with the Company as well as legal action.

5. Signatures

_____
Abdallah Shanti, EVP and CIO Region Americas

_____
Carey Cordes-McPherson, CISO

[SIGNATURES ON FILE]