VW CREDIT, INC. SYSTEM ACCESS POLICY

This VW Credit, Inc. System Access Policy ("**Policy**") applies if VCI gives a third party ("**Supplier**") access to VCI Systems to be used to provide services, products, or materials to VW Credit, Inc. ("**VCI**") in connection with the agreement between VCI and Supplier (the "**Agreement**"). This Policy contains specific requirements relating to access of VCI Systems that Supplier, its personnel, and any of its affiliates or subcontractors must meet in its performance of the Agreement. This Policy is incorporated by reference into the Agreement.

- Use of VCI Systems.
    - Supplier will use VCI Systems (as defined in the VW Credit, Inc. Third-Party Information Security Policy) in the performance of the Agreement.
    - VCI may terminate Supplier's access to VCI Systems at any time without notice to Supplier, its affiliates, subcontractors or any Supplier personnel.
    - if VCI terminates Supplier's access to VCI Systems, then Supplier will not be liable for any failure to perform under the Agreement that occurs as a result of the terminated access.
- Consent to Monitoring when Accessing VCI Systems.
    - VCI may monitor, record and analyze any access to, or data stored on, VCI Systems at any time.
    - Supplier consents to monitoring, recording and analysis. The Supplier is responsible for making sure Supplier personnel that access VCI Systems are aware of, and consent to, monitoring and recording.
    - Supplier, on behalf of itself and Supplier personnel, acknowledges that there is no express or implied right of privacy with respect to monitoring, recording and analysis.
- Login IDs for VCI Systems Access.
    - If applicable, VCI will assign a login code ("**Login ID**") to Supplier personnel who will have access to VCI Systems.
    - Supplier will not allow a Login ID to be shared with or used by an individual other than the assigned individual.
    - Supplier is responsible for all access to VCI Systems by any individual using a Login ID issued to any Supplier personnel.
    - Login IDs (and any other information on or obtained as a result of Supplier's access to the VCI Systems) are considered VCI's confidential information.
- Supplier Systems Used to Access VCI Systems. Supplier will:
    - be responsible for Supplier Systems (as defined in the VW Credit, Inc. Third-Party Information Security Policy) used to access VCI Systems.

- be responsible for making sure that Supplier Systems used to access VCI Systems are equipped with up-to-date anti-viral software that VCI reasonably determines is acceptable.
- prevent unauthorized access to VCI Systems through Supplier Systems.
- ensure that Supplier personnel do not use any virtual private network or other device ("**VPN**") to simultaneously connect machines on any VCI Systems to any machines on any Supplier Systems or third party systems, without:
- using a remote access method previously approved in writing by VCI;
- providing VCI with the full name of each individual who uses any such VPN and the phone number at which the individual may be reached while using the VPN; and
- ensuring that any computer used by Supplier personnel to remotely access VCI Systems will not simultaneously access the Internet or any other third party network while logged on to VCI Systems.

- Notification of Security Breach and of Unauthorized Access.
  - Supplier will notify VCI in writing within twenty-four (24) hours of any actual or reasonably suspected security breach and/or unauthorized access of VCI Systems or Supplier Systems used to access VCI Systems.
  - The notice of breach and/or unauthorized access provided to VCI must include (1) the reasonably expected impact of the security breach and/or unauthorized access on VCI and its customers; and (2) the remediation or corrective action to be taken with respect to Supplier Systems to prevent or mitigate any such security breach and/or unauthorized access.
- Third Party Restrictions on VCI Systems Access.
  - Access to VCI Systems may involve access to software or other technology licensed from third parties.

    Supplier and Supplier personnel will comply with all restrictions applicable to such third party software and technology.
- No Transmission of Harmful Material through VCI Systems Access.
  - Supplier will not transmit nor permit the transmission of any unlawful, discriminatory, threatening, libelous, defamatory, obscene, scandalous, inflammatory, pornographic or profane material through VCI Systems.
  - Supplier acknowledges that VCI intends to cooperate fully with law enforcement, regulatory or judicial investigations into any access to VCI Systems. This cooperation may include disclosure of the identity of, and the information transmitted or received by, individuals accessing VCI Systems.

  - If requested, Supplier will immediately remove access to VCI Systems of any Supplier personnel who violate the terms of this Policy, and ensure that any removed Supplier personnel are not involved in the performance of the Agreement.

- Removal of Data through VCI Systems Access. Supplier and Supplier personnel will not remove or retain a copy of any data or information obtained from, or as a result of access to, VCI Systems unless removal or retention is necessary for Supplier to perform its obligations under the Agreement.
- Disclaimer Regarding VCI Systems Access. ACCESS TO VCI SYSTEMS IS PROVIDED "AS IS" WITHOUT ANY WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.
- System Access Requirements for Affiliates, Subcontractors and Supplier Personnel. Supplier must obtain VCI's prior written approval to provide access to VCI Systems to any affiliate, subcontractor, or Supplier personnel of such affiliate or subcontractor.