



Nexteer Security Practices Document

DEFINITIONS

Workforce means : including but not limited to internal personnel, contractors, subcontractors, 3rd parties, 3rd party subcontractors

INTRODUCTION

Seller must accurately document all technical and organisational security measures and update this document accordingly. This document must be made available to Nexteer at the outset and subsequently as requested by Nexteer.

Seller must allow Nexteer to verify Seller's compliance with Nexteer's Security Practices Document prior to processing commencement.

ADMITTANCE CONTROL (PHYSICAL)

Seller will prevent unauthorised persons from gaining access to data processing systems with which Nexteer Personal Data is processed.

Seller will protect offices in which Nexteer Personal Data is processed by putting in place adequate physical security measures against access by unauthorised persons.

Seller will comply with the requirements outlined in the Nexteer Data Processing Agreement in connection with the provision of services to Nexteer Automotive.

ENTRY CONTROL (SYSTEMS)

Seller will prevent data processing systems from being used without authorisation. Seller will only grant workforce, access to applications which process Nexteer Personal Data to the extent they require it to fulfil their function.

Seller will ensure that the access control is supported by an authentication system.

Seller will comply with the requirements outlined in the Nexteer's Data Processing Agreement which will apply in respect of any Nexteer provided Software and Nexteer Systems used by Seller in connection with the provision of Services.

ACCESS CONTROL (DATA)

Seller will ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that Nexteer Personal Data cannot be read, copied, modified or removed without authorisation in the course of Processing and after storage.

Seller will only grant workforce authorisation to access Nexteer Personal Data who need the access to perform their functions in fulfilment of the Services.

Additionally Seller will only grant workforce the level of access (e.g. roles) required by such workforce to perform their respective functions in fulfilment of the Services.

Seller will ensure that only authorised workforce can access the Nexteer Personal Data.

If access is granted to any Nexteer provided Software and Nexteer Systems which is used in connection with the provision of Services then Seller will comply, and will procure the authorised workforce's compliance, with the requirements outlined in the Nexteer's Data Processing Agreement.

TRANSFER CONTROL

Seller will ensure that Nexteer Personal Information cannot be read, copied, modified or removed without authorisation during electronic transmission or transport, and that it is possible to check and establish to which 3rd parties the Nexteer Personal Data is transferred.

Seller will encrypt all Nexteer Personal Data if it is stored in an environment without physical access control or if it is stored or transferred outside Seller's logical and physical access control system.

Concerning the mentioned safeguards above...state of the art encryption tools and procedures should be used reflecting appropriately secure technology in order to ensure Seller's compliance with its obligations under Nexteer's Data Processing Agreement.

INPUT CONTROL

Seller will ensure that it is possible to check and establish whether and by whom Nexteer Personal Data has been inputted into data processing systems, modified or removed.

Seller may permit only authorised workforce to modify any Nexteer Personal Information within the scope of their function.

Seller must record any changes made to the Nexteer Personal Information, if such changes are not requested by Nexteer.

If Seller grants access to any application used in connection with the provision of the Services to Nexteer Automotive, Seller will, and will procure the authorised Service workforce's compliance with, the requirements outlined in the Nexteer's Data Processing Agreement.

JOB CONTROL

Seller will ensure that, in the case of commissioned Processing of Nexteer Personal Data, the data are processed strictly in accordance with the instructions of Nexteer.

Seller will take reasonable steps to ensure compliance with Nexteer's processing instructions.

AVAILABILITY CONTROL

Seller will ensure that Nexteer Personal Data is protected from accidental destruction or loss.

Seller will implement measures so that if there is a breakdown of the Services, Seller will be able to resume the Services within Nexteer's required timeframe.

Seller will comply with the requirements outlined in the Nexteer's Data Processing Agreement.

MULTI ENTITY SEPARATION CONTROL

Seller will Process Personal Information received from different clients or Service Recipients separately. Seller must ensure that in each step of the Processing the data controller of Personal Information can be identified. Seller will comply with the requirements outlined in the Nexteer's Data Processing Agreement.