PA ebusiness

mySalesDrive

Security Whitepaper v1

Contents

Glossary of Terms

CSP	Means the Cloud Service Provider selected by perform IT to host the mySalesDrive.com application, database, and associated Customer data.
Device Database	Means the device reference data used by mySalesDrive.com in order to calculate current-state TCO – and which is entirely separate from Project Data located in the Dedicated SQL Database Container. Device Database data is accessible to, and maintained by, perform IT – the originators of the mySalesDrive.com TCO calculator software. Device Database for Consultants located in United States of America is maintained directly by gap Intelligence – the provider of the data (printers, specifications, pricing etc.) in the US market.
Dedicated SQL Database Container	Separated Microsoft SQL server database file which is dedicated to a specific group of Consultants (perform IT clients / licensees) and located on a server in one of the available regions (CSP's data centre locations described in the Section 3.1). This file is the application database which contains Project Data, Customer information and information about Consultants along with their data. There are several Dedicated SQL Database Containers configured on each server. Each application instance (e.g. Trial, Europe, North America, Asia Pacific, OEM-1, OEM-2 etc.) has its own associated application database container.
Project (and Project Data)	Means a unique project created by a user (originating Consultant) within the mySalesDrive.com application that (a) contains Customer specific data (b) is by default only visible and editable by the originating Consultant (c) can be shared by the originating Consultant with other Consultants, as further described within Section 3.2.1, and (d) cannot be viewed by any third party.
Customer	Means any natural or legal person who tasks the Consultant to analyse and provide an optimisation proposal in the field of paper output management.
Consultant	Means a natural person who uses mySalesDrive.com for analysis and optimisation purposes.
TCO	Means Total Cost of Ownership – an industry-standard term used to describe the calculated overall cost of printing giving consideration to all known associated direct and indirect costs. The figure is intended to provide a basis for comparison and inform any subsequent purchasing decision.
WCF	Windows Communication Foundation – Communication platform for distributed applications.
IIS	Internet Information Services – Microsoft service platform designed for Windows servers to provide access to web content using communication protocols such as HTTP, FTP etc. This Windows service is essential for providing access to the ASP.NET and Silverlight applications.

1. Perform IT Security Principles

Perform IT is committed to providing software products that are secure for use in all environments.

mySalesDrive.com exclusively compiles, stores, and processes a number of imaging device metrics that are used to provide financial and environmental performance related analysis necessary to evaluate the effectiveness of a Customer's current-state printing environment and create optimisation proposals.

mySalesDrive.com does not use personal information, user information, print data, or any print job related information – and operates in a standalone environment without the need for connection to a Customer's computer network or IT infrastructure.

The data resident within mySalesDrive.com is stored in a third party secure cloud environment – conforming to IT security best-practice principles – and offering state-of-the-art security for data used by perform IT in providing TCO analysis.

Perform IT's selected secure cloud environment is certified to US Department of Defence Information Assurance (DIA CAP) and Cloud Security Model (DOD CSM) standards, Payment Card Industry Data Security Standards (PCI DSS), and has attained ISO 27001 Information Security Management accreditation.

2. About mySalesDrive.com

2.1 What is mySalesDrive.com?

mySalesDrive.com is a cloud-based software application to perform Total Cost of Ownership (TCO) assessment and generate quotes in day-to-day sales.

mySalesDrive.com has been developed by German-based software house perform IT – and represents the third generation of in-house developed Managed Print Services (MPS) software – originally 'ForSale' and most recently available under the brand name 'Vendor.'

mySalesDrive.com is available both in standard version and customised version according to perform IT client's request. Additionally, perform IT offers the possibility to provide a Dedicated SQL Database Container including own customised cloud application instance (e.g. mySalesDrive.com/OEM-1) on request. That application instance can be called from the customised landing page (e.g. mySalesDrive.com/CustomAppNameForOEM-1 or www.OEM-1-Domain.com/mySalesDrive) which includes the system requirements and start buttons for mySalesDrive.com cloud application and capture IT application for iPad as well.

2.2 How does mySalesDrive.com work?

mySalesDrive.com takes data regarding a Customer´s existing fleet of printing devices and – by reference to a comprehensive Device Database including machines, consumables and finishing equipment prices – calculates a related current-state TCO. The accuracy of the TCO can be further refined by substituting database pricing values with 'actual' Customer values – including software application fees, financing costs, service and support pricing, – and any other related charges – into the final calculation.

The tool includes further functionality that is key to understanding current-state solution design. This includes the ability to plot current devices, departments, numbers of users, and infrastructure onto an image of the Customer's floorplan. Fully understanding current-state device geography – and how devices form part of organisational workflows – allows the formulation of an optimised layout based on 'rules' (the Customers Print Policy) agreed with the Customer. Current-state and future-state floorplans can be compared to ensure improved ergonomics and workability – but most importantly – mySalesDrive.com uses future-state floor plan data (devices, configurations, volumes, etc.) to calculate a future-state TCO.

The software then is able to generate a report in Word, Excel, or PowerPoint that compares current-state and future-state TCO – and uses this calculation to highlight the extent of any potential cost savings that could be realised by the Customer.

2.3 What Data is collected by mySalesDrive.com and what is it used for?

mySalesDrive.com includes a universal import engine that is able to identify data gathered from commonly-used print monitoring and/or fleet management software (including but not limited to Print Audit) and use this to automatically generate a TCO. Where a Customer has not deployed such an application – or not all devices are connected to it – then data can be gathered manually using information provided by the Customer and subsequently compiled into a spreadsheet. Alternatively, Consultants can conduct physical site audits using a tablet-based App specifically designed to be used in conjunction with mySalesDrive.com, the 'capture IT' module for iPad. Resultant data can then be uploaded into the mySalesDrive.com application via an Internet connection.

Data gathered includes the items detailed within section 2.3.1. However, not all data is essential to achieving a TCO calculation, some data is used simply for device identification, and some is specific to the future-state design process.

It goes without saying that the integrity and accuracy of both current-state and future-state TCO calculations – and the ability of a Consultant to carry out an effective optimisation exercise – are compromised if access to sources of data are limited. As such, it is imperative that Customers concerned about data security are fully informed regarding the potential impact that individual limitations may have on the value of their consulting exercise.

Specific Data	Used For	Degree of necessity
Device IP address	Device reference/ID point	Optional
Device MAC address	Device reference/ID point	Optional
Device serial number	Device reference/ID point	Preferred
Manufacturer	TCO Calculation	**Must-have**
Model variant	TCO Calculation	**Must-have**
Finishing options and add-on	TCO Calculation	Preferred
Meter reading or estimated monthly volume	TCO Calculation	**Must-have**
Purchase price/asset value	TCO Calculation	Preferred
Installation data/manufacture date	TCO Calculation	Preferred
Contract/service cost	TCO Calculation	Preferred
Device ownership status (leased/owned/rented)	TCO Calculation	Preferred
Device location	Optimisation	Preferred
Department name	Optimisation	Optional
Building name	Optimisation	Optional
Floor number	Optimisation	Preferred
Floor plan	Optimisation	Optional

2.4 Summary

- mySalesDrive.com is a cloud-based software application to perform an assessment of a Customer´s current-state printing environment, and to design an optimised future-state solution.
- mySalesDrive.com requires information about the Customers current-state devices in order to calculate a TCO. The data upon which this is based may originate from a number of different sources, including (i) a report generated by any device monitoring application currently being used by the Customer or which the Consultant might – with the Customer's permission – temporarily deploy (ii) from a physical audit of the Customer´s environment conducted by a Consultant (iii) from other sources of data that the Customer might have e.g. monthly invoice data from the incumbent equipment supplier.
- mySalesDrive.com is a standalone software tool that does not connect to the Customer's network

3. Security Information

3.1 Overview

mySalesDrive.com is a cloud-based software solution developed by German-based software house perform IT (www.performit.net). The solution makes use of a cloud platform provided by a leading cloud service provider (CSP) from data centres located in Frankfurt (Germany), Oregon (United States of America), and Sydney (Australia). User accounts are assigned to the most suitable data centre by perform IT´s own mySalesDrive.com support team, based on the user's geographical location (for details please see the table below), and -if necessary – formal testing of the integrity of the link to the preferred data centre prior to the assignment.

Location	Data Centre
United States of America, Canada, and South American countries	Oregon (United States of America)
Australia, China, Hong Kong, Japan, New Zealand, Singapore, East Asia and Pacific Rim countries	Sydney (Australia)
Europe, Middle East, South Africa and Central Asian countries	Frankfurt (Germany)

The CSP was selected by perform IT as its preferred hosting service provider as it offers a highly secure cloud computing environment.

The CSP operates a global cloud infrastructure used to provide a variety of basic computing resources, including processing and storage. The CSP's global infrastructure includes the facilities, network, hardware, and operational software (e.g., host OS, virtualisation software, etc.) that support the provisioning and use of these resources. The CSP's global infrastructure is designed and managed according to security best practices, as well as a variety of security compliance standards.

This document provides an overview of the current security infrastructure, procedures, and practices related to mySalesDrive.com, the application provider perform IT, and the CSP – and is intended as a guide to Customers in relation to the security provisions that apply to data captured – and subsequently processed by dealers and manufacturers – using the mySalesDrive.com application.

3.2 Application Security and Administration

3.2.1 Project Data

Project sharing security is provided using the permissions stored in the SQL database of mySalesDrive.com. By default, only the original Project owner (Consultant) is able to see individual Project/Customer related data. Functionality exists within the mySalesDrive.com application to enable Projects to be shared between colleagues – primarily to bring efficiency to initial data gathering activity e.g. for larger Customer projects that might involve multi-country, multi-site audit processes. This capability can only be enabled by the project owner if a sharing feature for one of the levels – Group, Country or Globally – is activated by mySalesDrive.com administrators.

3.2.2 Segregation of Customer Data

perform IT client's Customer's data is physically located in one of the Dedicated SQL Database Containers with the associated file server folders dependent on the location of each user's assigned CSP data centre. Although the Project Data of different Customers from the same region could be stored in the same Dedicated SQL Database Container, it is protected against any unpermitted access by using (i) Windows permissions (ii) IIS permissions and security (iii) WCF service permissions and secured methods (iv) SQL database permission and limited access rights (v) Framework for protection against SQL injection or similar hacker attacks (vi) mySalesDrive.com Project user (Consultant) rights based on database's referential integrity in combination with the software specific security architecture and methods implemented by perform IT (vii) for estimation purposes, anonymised average numbers can be only retrieved by Consultants if at least 3 projects within the same Dedicated SQL Database Container could be found for using as a data source in order to avoid any conclusion concerning Customer's Project Data.

3.2.3 Application Administrators (Software Vendor Side)

perform IT has access to the database files on the lowest administration level for backup and maintenance purposes. Only a limited number of employees have access to the database on the lowest level. In order to create new accounts, the perform IT support team uses the standard mySalesDrive.com admin frontend webpage.

3.2.4 CSP and Application User Password Security

Access to the CSP cloud is controlled through the application of a number of protocols and safeguards. These include:

- Remote desktop connection is only possible from the static perform IT office IP address.
- The CSP cloud password is between 10 – 20 signs (currently 107-bit protection) and governed by Microsoft best-practice guidelines (i.e. passwords consist of upper and lower case letters, numerical characters, and non-alphanumeric characters). Valid whole words are not allowed. Passwords are changed regularly. The same principle applies to SQL database accounts and Windows server administrator accounts.
- Passwords (including CSP access credentials) are stored in a secure encrypted database. This database is located within perform IT's internal network and encrypted using a password and special key file.
- All printed security documents are assigned to a specific perform IT employee who is responsible for its safe-keeping. Employees are not allowed to make copies or share documents with other individuals.
- perform IT uses network-wide endpoint protection hardware and software with firewall – including file-system protection against viruses and hacker attacks (i.e. web-protection, mail-protection, network-protection, p2p-protection, IM-protection, user-behaviour-protection, and script-protection).
- A restricted number of named individuals from perform IT have access to the CSP servers. Each named individual has signed a Non-Disclosure Agreement as part of their contract of employment.

mySalesDrive.com application user passwords are administered by perform IT mySalesDrive.com support team. Requests for account allocation are made to a dedicated e-mail address. Consultants are able to change their password at any time by themselves. All passwords are stored encrypted in the mySalesDrive.com system using a one-way encryption method. There is no way to decrypt a password, not even for the perform IT administrators.

3.3 CSP IT Security Standards

The IT infrastructure that the CSP provides to perform IT is designed and managed in alignment with security best practices and a variety of IT security standards, these include:

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 27001
- ITAR
- FIPS 140-2
- MTCS Level 3

In addition, the CSP's cloud platform meets several industry-specific IT-Security standards, including:

- HIPAA
- Cloud Security Alliance (CSA)
- Motion Picture Association of America (MPAA)

3.4 CSP Physical and Environmental Security

3.4.1 Overview

The CSP's Data Centres are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilising video surveillance, intrusion detection systems, and other electronic means. Authorised staff must pass two-factor authentication a minimum of two-times to access Data Centre floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorised staff.
The CSP only provides Data Centre access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of the CSP. All physical access to Data Centres by CSP employees is logged and audited routinely.

3.4.2 Fire Detection and Suppression

Automatic fire detection and suppression equipment is installed at the Data Centres. The fire detection system utilises smoke detection sensors in all Data Centre environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe double-interlocked pre-action, or gaseous sprinkler systems.

3.4.3 Power

Data Centre electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours per day, seven days per week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads. Data Centres use generators to provide back-up power for the entire facility.

3.4.4 Climate and Temperature

Climate control maintains a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data Centres are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels.

3.4.5 Management

The CSP monitors electrical, mechanical, and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

3.4.6 Storage Device Decommissioning

When a storage device has reached the end of its useful life, the CSP procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorised individuals. The CSP uses the techniques detailed within DoD 5220.22-M ('National Industrial Security Program Operating Manual') or NIST 800-88 ('Guidelines for Media Sanitization') to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

3.4.7 Business Continuity Management

The CSP has designed its systems to tolerate system or hardware failures with minimal customer impact.

3.4.8 Availability

Data Centres are built in clusters in various global regions. All Data Centres are online and serving customers; no Data Centre is 'cold'. In the event of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a Data Centre failure, there is sufficient capacity to enable traffic to be load-balanced to remaining sites.

3.5 CSP Network Security

3.5.1 Secure Network Architecture

Network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule-sets, access control lists (ACLs), and configurations to enforce the flow of information to specific information system services.
ACLs, or traffic flow policies, are established on each managed interface, which manage and enforce the flow of traffic.

3.5.2 Secure Access Points

The CSP has strategically placed a limited number of access points to the cloud to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. These customer access points are called API endpoints, and allow secure HTTP access (HTTPS).

To support customers with FIPS 140-2 requirements, the CSP's Virtual Private Cloud VPN endpoints and SSL-terminating load balancers in the CSP GovCloud (US) operate using FIPS 140-2 level 2-validated hardware.

In addition, the CSP has implemented network devices that are dedicated to managing interfacing communications with Internet service providers (ISPs). The CSP employs a redundant connection to more than one communication service at each Internet-facing edge of the CSP's network. These connections each have dedicated network devices.

3.5.3 Transmission Protection

The Data Centre provides a CSP access point via HTTP or HTTPS using Secure Sockets Layer (SSL), a cryptographic protocol that is designed to protect against eavesdropping, tampering, and message forgery.

3.5.4 Corporate Segregation

Logically, the CSP's production (customer) network is segregated from its corporate (administrative) network by means of a complex set of network security/segregation devices. CSP developers and administrators on the corporate network who need to access the CSP cloud components in order to maintain them must explicitly request access through the CSP ticketing system. All requests are reviewed and approved by the applicable service owner. Approved CSP personnel then connect to the CSP network through a bastion host that restricts access to network devices and other cloud components, logging all activity for security review. Access to bastion hosts require SSH public key authentication for all user accounts on the host.

PA e business

PAE Business
(UK, Ireland, EMEA Headquarters)
3 Tannery House, Tannery Lane
Send, Guildford
Surrey, GU23 7EF
United Kingdom

Telephone: +44 (0) 1483 726 206

Sales@paebusiness.com
Support@paebusiness.com