Dealership I.T. Guidelines

TOYOTA MOTOR CORPORATION AUSTRALIA

Last updated: January 2010

TOYOTA MOTOR CORPORATION AUSTRALIA

DEALERSHIP IT GUIDE

VERSION **1.0**

LAST UPDATED **20 JANUARY 2010**

VALID UNTIL **30 SEPTEMBER 2010**

TABLE OF CONTENTS

TABLES AND FIGURES

Introduction

This is the first release of a consolidated document that TMCA hopes will provide advice and support to dealerships in the IT area.

IT is becoming an increasingly important facilitator of our business. The effective and timely storage, capture and distribution of key financial, product, technical, and pricing information is critical to operating an efficient competitive business.

Toyota Australia understands that version 1 will not provide all the IT information you as a dealer, will require. It is our intention to enhance and improve this service in line with your feedback and requests.

If you have any comments or additional requirements - please complete the feedback form located at the end of this document.

1 Executive Summary

1.1 Purpose of the Guide

The TMCA Dealership IT Guide is designed to help you plan, install and manage a sustainable, reliable and secure IT environment that provides you with a good return on your IT investment.

The Guide will facilitate both your **strategic** and **operational** IT business plans by helping you to:

- Understand the IT investment requirements and how you can leverage IT to take advantage of TMCA's initiatives;
- Plan and budget your IT investments to maximise the useful life of your IT equipment;
- Follow best practices in the industry to manage and maximise the return on your IT investment;
- Understand the value proposition of Toyota Motor Corporation Australia's (TMCA's) IT strategies, directions and initiatives, and how they can enhance your franchise value

After reading this document, you will be able to answer the fundamental Information Technology (IT) questions facing TMCA dealers today. Namely,

- **What practices will optimise your investment?**
- **How can you support/protect your investment?**
- **What investment is required in each area of your dealership?**
- **What skills are required to maximise your IT investment**

1.2 Disclaimer

The IT Guide is designed to help you plan, manage, leverage and get a good return on your IT investments. Although the recommendations provided are based on extensive research and experience, there is no guarantee that they are the best ones for all dealership environments. In the equipment recommendations, TMCA only provides technology specifications. It is up to you to work with your technology partners and/or vendors to decide on the brands and makes of the equipment to purchase. TMCA has no obligation to support practices or use of equipment outside of the recommended set, as layout in this document. It is your responsibility to make sure that the equipment you have chosen will be compatible with TMCA applications and will enable you to participate in TMCA initiatives. To the extent permitted by law, TMCA is not liable for any loss which is directly or indirectly caused by any act or omission based in whole or in part on any recommendation contained in this IT Guide.

In addition, technological developments occur rapidly and it is important that TMCA and its dealers ensure that their IT systems maintain currency so that they can continue to serve the needs of TMCA and its dealers and, ultimately, potential customers. This includes the need for evolving technological capabilities and the need to adopt the latest strategies to protect the security of the TMCA and dealer IT systems. TMCA reserves the right to make changes to this IT guide at any time in its absolute discretion although you should also make yourself aware of any changes to best practices that are relevant to your dealership.

1.3 Target Audience

The intention *of this document* is not to make you an IT expert or to divert you from the fundamentals of running a profitable dealership, namely, selling and servicing vehicles. However, IT can facilitate your efforts. It is important to get the most out of your IT tools and investments.

Who should read this document? ***This Guide is essential reading for the person or persons directly, and fiscally, responsible for planning and managing your dealership's***

IT environment. Our recommendation is that you, the dealer principal or general manager, also read the entire document at least once. At a minimum, we strongly recommend that you

a) Read this Executive Summary. This will enable you to understand the scope of the Dealership IT Guide and the reasons why it has been created.

b) Review Section 2, Dealership IT Guidelines. This will provide you with an overview of the guidelines and recommendations designed to help your dealership optimise its IT investment.

c) Review Appendix B. This will give you a checklist of hardware, software and networking specifications and requirements for your dealership and will allow you to assess your "IT readiness" to leverage the TMCA e-Business initiatives to benefit your dealership.

d) Assign appropriate members of your staff (e.g. your controller, sales manager, IT manager and/or Dealer Technology Administrator) to read this Guide in its entirety and then set aside some time to answer the following 8 *"Are We 'IT Ready'?"* questions (once you and/or your designate(s) have read the Guide).

Are We 'IT Ready'?	
	1. Are we in compliance with the guidelines specified in the IT Checklist? If not, where are the gaps and what are the plans to fill them?
	2. Have we adopted best practices in the management of our IT investment?
	3. What IT investment should we be planning for in 2010, 2011?
	4. Is our dealership 'IT ready' to leverage the TMCA e-business initiatives? If not, how and where can we improve?
	5. Is our Dealer Technology Administrator capable of handling the responsibilities outlined in Section 2.5 required? If not, what additional training is required?
	6. Is our current technology partner, or internal IT staff, capable of providing the type of service outlined in Section 2.5? If not, what needs to be done?
	7. Is the data in the dealership protected from unauthorised electronic access and viruses?
	8. Is our backup (or business resumption) plan consistent with the Guide's recommendations? If not, what needs to be done?

Table 1 - Are We 'IT Ready'?

Making the right IT investments can help you improve your business' bottom line. The Dealership IT Guide will greatly assist you in this respect.

1.4 Your Strategic and Operational Planning Guide

This document should be the basis for on-going assessments of your dealership IT needs. We urge you to make it a part of both your strategic and operational business plans.

You should consult the Dealership IT Guide prior to…

- Investing in IT hardware or software
- Disposing of old IT equipment
- Renovating/rebuilding your facilities
- Hiring personnel

- Contracting the services of third party vendors
- Implementing data protection strategies.

The Dealership IT Guide is applicable to Toyota dealerships of all sizes. Appendix B, outlines the hardware and software requirements for all dealer categories, so your dealership will benefit regardless of its dealership weighting.

Please note that this guide does not address privacy issues regarding the collection of customer data using IT applications. To get more information about data privacy, please refer to the Dealer Kaizen Committee.

1.5 IT as an Investment

This Guide will enhance the value of IT in its ability to support (run the business), enable (grow the business) and drive business changes (transform the business). By following our recommendations, you will be able to leverage the many TMCA initiatives intended to:

- Make your staff more efficient and productive;
- Expand your market share;
- Enhance customer relationships and satisfaction.

IT investment is more than just buying a number of servers and personal computers (PCs), and installing them on your staff's desktops. The effectiveness of any productivity tool is dependent on how it is used. A sound IT investment considers how to optimise hardware, software *and people* resources. Leveraging resources both internal and external to your dealership(s) is a key to maximising your ROI. For example, connecting your dealership's computers via a local area network (LAN) enables collaboration and sharing of internal resources. Connecting over a wide area network (WAN) enables access to external applications and resources to leverage the investments, research and development of TMCA and other business partners.

IT investment is not static. As with all technologies, IT is constantly changing and can become obsolete as newer innovations are introduced or as business needs change. Your IT investment should not be looked upon as a one-time event. You should reserve a portion of your annual budget to keep your IT environment current and viable.

With many installations, it is not unusual to find that costs incurred after the initial deployment can be up to 80% of your overall IT investment. It is therefore critical to effectively manage your IT life cycle costs through complementary investments in training people, streamlining processes, including business integration and asset management processes, and acquiring technologies that are easy to manage, service and support.

It is recommended to assign 12% to 18% of your IT budget to support functions.

1.6 Document Layout

This document has been organised into 8 sections:

- Section 1 – Executive Summary (this section) is designed to give you a quick overview of this document and to enlist your support and commitment to participate in the TMCA initiatives.
- Section 2, Dealership IT Guidelines is designed to help you understand the scope of your IT investment requirements and why they are needed; and to provide you with a list of IT investment management best practices so that you can optimise your investment.

- Section 3, Business Applications outlines the TMCA strategies and the benefits of the various initiatives. This will give you a clear understanding of the initiatives TMCA is rolling out and how you can take advantage of TMCA's investments to achieve our mutual business objectives.
- Section 4, Sample Computer and Internet Use Policy is intended to provide you with a list of "Do's" and "Don'ts" that you can customise to direct your staff on what is appropriate and inappropriate use of your computer and network resources.
- Section 5, Contact List gives you the major contact names and numbers from TMCA, and other business partners.
- Section 6, Technology Partner Selection Guide is intended to provide you with a set of questions and considerations to help you qualify and select the right technology partner for your dealership, if you are looking for an outside technology partner to support your dealership or complement your in-house IT staff
- Section 7, Role of the Dealer Technology Administrator itemises the typical tasks and responsibilities of the Dealer Technology Administrator (DTA), a role that factors prominently in the support of your dealership's IT environment. Every dealership should have a DTA, although in many cases the role may be combined with other dealership responsibilities.
- Section 8, Glossary gives you a brief description of key terms used in this document to aid your understanding.

1.7 Keeping the Guide Relevant

A key challenge in creating the Dealership IT Guide is to maintain relevance beyond its initial release. This means not only providing guidance on new IT equipment purchase decisions, but also providing an ongoing picture of the IT investment requirements that dealers should expect over the next few years.

The IT Guide will be updated annually to keep the publication current and relevant, and to take advantage of the benefits that newer technologies may provide.

Every year, as you purchase new IT equipment, you may want to consider introducing them in the more processing demanding or more visible areas, such as in the Service Advisor area or in the Sales Showroom, and cascade the older equipment to less demanding areas, such as the general office.

Our direction is to keep on updating the standards in this Guide so that you can take advantage of the functions and price/performance of new technologies. Unless necessitated by new, unforeseen business requirements, we will avoid making changes that will require significant new investments or create incompatibilities in your IT infrastructure. In future, should a major revision to the specifications be necessary, every effort will be made to ensure that any IT investments based on previous Guide recommendations will be protected as much as possible.

1.8 FAQs

The Dealership IT Guide was created to provide a consolidated picture of the on-going IT investment requirements that dealers could expect over the next several years. The following are answers to some of the questions frequently asked:

Q **How did you come up with the recommended specifications?**

A Our recommended specifications are based on a number of careful considerations, including:

- What is generally available in the market place?
- What are the projected product life cycles of the hardware and software technologies under consideration?
- What are the projected resource requirements (e.g. processing power, hard-drive storage) to enable the dealers to leverage current and emerging business initiatives from TMCA and its strategic business partners effectively?

- What is the likelihood that the recommended equipment will be able to meet the average user requirements over the 4-year "evergreening" life cycle?

The "business-grade" equipment chosen is generally not the top-end or the latest leading edge offering in the marketplace. The recommendations are typically based on stable and proven technologies. Reliability, good price/performance and investment protection are the key selection criteria.

Q **Have other Toyota distributors published similar Guidelines?**

A The concept and large portions of this document come from Toyota Canada's IT Blueprint. Parts of their IT Blueprint are now adopted by other Toyota dealers in the US and Europe.

Q **If my IT equipment is below the recommended specifications, am I expected to upgrade my hardware inventory immediately?**

A If you continue to use equipment that is below the recommended levels, you should be prepared that it may no longer work at some point in time, and that only limited support will be available from tSupport. However, we advise against "retrofitting" older PCs to newer specifications (such as replacing the hard-drive, motherboard or even the Operating System). Major upgrades of existing equipment such as these can introduce other complications and incompatibilities. Often, it is better to replace the equipment altogether, especially when considering that hardware and software costs are only a small part of the total cost of ownership when factoring in support costs, impact on user productivity and missed opportunities.

Your best course is to follow the 4-year "Evergreen" policy by acquiring/replacing at least 25% of your total IT equipment every year, starting with the old equipment.

Q **Why is a 4-year "Evergreening" Cycle being recommended?**

A The estimation on the useful life of the IT investment is dependent on several factors, including the intended purpose of the investment, the speed of technological change, the evolving business environment and strategic initiatives to enhance competitive position. Our objective with the Dealership IT Guide is not to keep pace with the fast rate of technology change, but to ensure TMCA and its dealers are able to stay competitive in the marketplace by leveraging the benefits of IT. We believe an "Evergreening" Cycle is essential in meeting this objective.

Q **Does the Dealership IT Guide apply to dealerships of all sizes?**

A Yes. The Dealership IT Guide is designed to help dealers plan, manage, leverage and get a good return on their IT investments regardless of dealership size. You will find the guidelines and best practices useful and practical, regardless of your dealership size. The guidelines should be viewed as minimum requirements. Any variation on the guidelines should be made with a view to adding, and not reducing functionality.

Q **What are the consequences to dealers of not complying with the guidelines provided in the Dealership IT Guide?**

A The consequences of failing to meet the guidelines are more performance and support related, and the inability to capitalise on the benefits of TMCA business initiatives. This will have a direct bearing on the operational efficiencies, and hence, profitability of your dealership. To avoid potential problems, dealers are strongly encouraged to comply with the guidelines.

Q **Some dealers feel that TMCA's policy is to download more and more costs to the dealers. Why does TMCA not share in more of the costs to implement its technology initiatives?**

A A perception with some dealers is that TMCA's plan to reduce paper communication will mean increased paper costs for dealers. Actually, TMCA's goal is to increase the speed

and effectiveness of communications and information dissemination across the entire dealer network. Electronic communications is far more efficient than paper-based communications.

Q **What if several of the TMCA initiatives that require hardware and/or software upgrades by dealers do not pan out?**

A TMCA has gone to considerable lengths to pilot test its technology initiatives before launching to the dealer network. The pilots have involved dealers in every stage of project development. TMCA has made significant investments in product development and shares in the risks and potential benefits. TMCA will continue to invest in proof-of-concept efforts to minimise the potential exposure to itself and its dealers.

Q **How can we be assured of getting a good return on our IT investments?**

A Acquiring IT equipment and setting up the proper infrastructure in accordance to the recommendations in the Guide are only part of the equation. Your staff must have the competence and skills to use the tools to their advantage. This includes providing adequate training and integrating the processes introduced by the TMCA initiatives into your daily operation. Competent technical support, either in-house or through a third-party technology partner, is essential to the success of your dealership.

2 Dealership IT Guidelines

2.1 Scope

This Section defines the requirements and guidelines for you to leverage the TMCA initiatives. Although it includes a high-level discussion on the IT technology requirements, specific equipment specifications and/or vendor selections are not part of the recommendations. It is up to you, your IT staff and/or technology partner to determine your specific needs and invest in the required equipment, processes and skills accordingly.

This document focuses on the IT requirements to access and/or interface with applications and services that support the TMCA initiatives. It can serve as a good foundation or starting point for your overall IT requirements planning. We urge you to take any unique requirements into serious consideration before you finalise your IT infrastructure.

2.2 General Guidelines and Best Practices

Managing your IT investment should not mean reinventing the wheel. Here is a snapshot of some IT 'best practices':

1. Do not treat your IT investment as a one-time event. You should:
    - Review your IT portfolio every year.
    - Smooth out the peaks and valleys of your investment by adopting a 4-year 'evergreening' strategy that involves upgrading one-quarter of your IT equipment annually.
    - Acquire new equipment with functionality and price/performance that meet your evolving business requirements
    - Purchase only IT equipment that meets or exceeds the 'recommended specifications'.
    - Dispose of obsolete equipment that no longer serves your needs or has become too expensive to upkeep or maintain.
2. In addition to capital equipment, you should also invest in:
    - Integrating the new processes into your daily business operations to capitalise on the new ways of doing business.
    - Assigning *12% to 18%* of your IT budget to staff training and support functions, including
        - People training *(e.g. Product & Service Advisors as well as Technicians)* so that your staff know how to use IT equipment in a productive manner
        - A support infrastructure with a Dealer Technology Administrator in place (with proper backup) to manage and co-ordinate all IT-related activities in your dealership and to provide first level support to your staff.
    - In-depth IT skills, either in-house or from your technology partner, to keep your IT environment current and operational, and to help you resolve any problems.
    - Sound IT practices, such as performing regular anti-virus protection updates and backing up critical business data.
3. Maximise the return on your IT investments by:
    - Differentiating between the 'useful life' and 'economic life' of your investment. The useful life of most IT equipment should be at least as long as its economic life.
    - Employing a "cascading" strategy to re-deploy older IT equipment in user areas with less demanding IT requirements.
    - Being a close follower, not a pioneer, in adopting new technologies.

- Ordering workstations with spare capacities to meet future requirements.
- Spelling out a computer and Internet usage policy for your dealership to prevent abuse of privileges.
- Following TMCA recommendations and standards, including Dealer Website standards, with your IT investments.

4. Manage your IT assets effectively by:
   - Maintaining detailed records of your IT assets to help manage your cascading and refurbishing programs. Keeping your IT environment simple to facilitate supportability. You should strive for an environment with
     - a common platform for your hardware and software configurations
     - a common workstation image
     - as few vendors as possible.
5. Make sure that you have an optimum computing and networking environment. (Examples provided below to show what some recommendations might be)
   - Install a local area network (LAN) with a router/gateway device to enable multiple PCs to share a single ISP connection.
   - Monitor utilisation of your both your ISP connection and DAN connection to make sure that it has sufficient bandwidth to support access to external applications and resources.
   - Maintain an up-to-date Network Diagram of your IT environment. An accurate Network Diagram will facilitate asset and network performance management as well as problem diagnosis and resolution.
   - Upgrade the speed of your LAN to 100 Mbps once most of your computing devices have 10/100 NIC cards installed. The higher speed LAN will enable faster transmission and exchange of information.
   - Optimise hard-drive disk space by regularly archiving obsolete e-mail messages, deleting temporary and unnecessary Internet files and using PC system tools to do disk cleanups.
   - Optimise the performance of your workstations by using a PC utility program, such as the Windows Disk Defragmenter Accessory program or Norton Utilities to consolidate and organise hard-disk space on user workstations.
   - Use the “forwarding” facility to re-direct or consolidate e-mail if you have multiple e-mail accounts.
6. Ensure that you have an adequate support infrastructure to keep your IT environment viable and effective.
   - In the absence of in-house technical resources, contract the services of a local technology partner.
   - Screen the services of potential technology partners by using the Technology Partner Selection Guide included in this Dealership IT Guide.
   - Appoint a Dealer Technology administrator, e-Learning co-ordinator and email administrator to support end users in your dealership. The administrator functions can be provided by the same person or assigned to different individuals.
7. Keep your IT environment safe and secure
   - Be careful in granting, and vigilant in maintaining, your staff’s access rights to TMCA applications. You or your designate must decide who in your dealership is privy to what information. Furthermore, the user records of former employees should be deleted immediately upon termination.

- Ensure you have an anti-virus program installed and active in every server and workstation in the dealership.
- You should have a current subscription of the anti-virus program enabling regular updates, which will ensure that your dealership is protected against the latest viruses.
- Use a facility provided by the Anti-Virus program to create Rescue Disks. The Rescue Disks will enable you to recover if your computer unfortunately gets infected. Keep the Rescue Disks in a safe place.
- Never open an attachment from an e-mail message if you do not know the Sender. Be especially suspicious of files with extensions (last 3 characters) of .PIF, .BAT, .COM, .EXE, or .VBS, even if it is from somebody you know.
- Do not download files from the Internet unless you know it is from a reputable source.
- Use the Anti-virus Program to scan floppy disks or CDs that somebody else gives you prior to opening or saving any files on your computer.
- Schedule the Anti-virus Program to automatically perform regular scans on all your hard drives. Fix any problems it may detect.
- Permit all workstations on your LAN to access the Internet but deny ALL access from the Internet into your network.
- Instead of monitoring your own ISP connection, consider subscribing to a remote or centrally managed firewall service.
- Ensure wireless LANs are installed with proper security measures and control.

8. Protect against physical and environmental elements
   - Plug all computer equipment directly into wall outlets with proper grounding. To prevent overloading, ensure any devices sharing an electrical circuit do not cause total amperage to exceed 80% of the circuit's amperage rating.
   - Consider installing a surge protector at the main circuit breaker to safeguard against sudden high voltage electrical power surges.
   - Place each laser printer on its own dedicated electrical circuit.
   - Consider including an Uninterruptible Power Supply (UPS) in the server configurations. An UPS provides power to the servers for the time required to restore primary power.
9. Enable business continuity
   - Backup files on auxiliary devices, such as tapes, CDs or DVDs, if possible. Your backup process should include careful labelling and storage of backed up information. Test your restoration process to ensure that it works.
   - Store a backup copy of your vital files (e.g. financial and customer records) off-site.
   - Implement a firewall/gateway solution that includes a secondary high-speed connection as a backup should the primary high-speed Internet connection (DSL or Cable) fail. Alternatively, spread out the bandwidth of the two sources evenly among the network resources so as to increase internet access speed overall. Computers can be set up with a primary and secondary gateway so that when one fails, the machine will automatically seek the secondary access point.
   - Have a computer emergency response process in place to handle crisis situations.

2.3 Workstation, Server and Printer Guidelines

2.3.1 Workstation Guidelines and Considerations

Workstations probably represent the lion's share of your IT equipment investment.

In Appendix B, we specify the hardware, software and networking recommendations. You should consult your DMS vendor regarding the requirements and configurations for the number of workstations and printers required for each area within your dealership.

This is a guide for your IT investment. When you purchase new workstations, you should only acquire equipment that conform to or exceed the current hardware and software specifications.

2.3.2 Tips to Extend the Useful Life of Workstations

The following are some tips that will help you extend the useful life of your workstations:

Cascading

"Cascading" is a process that is often used to re-deploy or migrate IT equipment down the hierarchical asset portfolio to exploit less demanding requirements. This is an effective process to extend the useful life of IT equipment when their functions can no long satisfy the needs of current users. "Cascading" implies that the migration of one PC may set off a chain of other displacements.

You may consider using this process to reduce your overall IT investment. With this strategy, you will usually only purchase systems that meet your high-end requirements, or systems that give you the most visibility and/or payback, and re-deploy existing systems down the hierarchy (e.g., out of the Showroom into the Sales Manager's office). In time, all your workstations will have higher functional capabilities than if you were to just buy low-end systems for everybody.

A word of caution with this process: some cleanup and refurbishment is usually required before cascading the equipment. Also, this "hand-me-down" style of asset management may require you to manage the expectations of your staff.

Order workstations with spare capacities

Often workstations (or PCs) become obsolete because they don't have the functionality or capacity to keep up with the requirements of new operating systems, applications, user productivity and processing (e.g. multiple simultaneous application windows), and networking. The main factors are usually the processor speed, RAM (Random Access Memory), or hard drive capacities, because they are not as simple to upgrade as other "plug and play" components (e.g. monitor). For example, replacing the hard drive usually means burning in a new systems image and copying over all the user data.

To help minimize the need for such upgrades, the accepted practice is to order workstations with higher processor speed, RAM and hard disk capacities than the immediate requirements. The additional cost usually is not significant, and you will be able to enhance user productivity and extend the useful life of the workstations. The recommended configurations already include some spare capacity to accommodate future TMCA initiatives. If you have additional requirements, then you may want to allow for larger processing capacity.

2.3.3 Server Guidelines and Considerations

As far as TMCA is concerned, the only servers required in the dealerships are your DMS (Dealer Management System) servers to support daily dealership operations. These servers are configured and provided by your DMS vendor. Accordingly, you should consult your DMS vendor regarding the requirements and configurations.

You may have other server requirements to support in-house IT processing, such as standalone accounting, and/or payroll applications, or to support other OEM and business partners' requirements. These are outside the scope of this IT guide. It is your responsibility to determine your server requirements for such circumstances.

2.3.4 Printer Guidelines

Printer requirements are dependent on how comfortable your staff is with getting information right off their desktop displays, as opposed to working from hard copies. We

leave it up to you and your technical support to determine how the printers will be shared, how many you may need, or where they should be located.

Studies have shown that it would be to your benefit to share printing facilities through network based printers wherever possible. If you require individual printers at workstations, standardise the brands and models for these printers. This allows you to consolidate supply purchases of ink and toner to minimize different cartridge models and take advantage of bulk purchases.

Since printers have so many moving parts, it should be emphasized that they be replaced every 4 years. Older printers will consume more supplies than newer ones while delivering poorer quality printouts and increased maintenance costs as they age.

As *vendors* introduce new technologies to increase printer functions and/or lower purchase prices, some of the new proprietary technologies may not be compatible with current TMCA and non-TMCA applications. When purchasing new makes or models of printers different from those installed in your dealership, it is your responsibility to first verify that the new printer can interface with the intended business applications. Before committing your purchase, you should ask your technology partner to supply you with a demo unit to make sure that you can test printing forms and reports from your applications without problems.

2.4 Network Guidelines

2.4.1 Networking Requirements

The IT infrastructure in a dealership typically contains three types of networks:

1. A Local Area Network (LAN) with cabling system to connect the workstations, servers and printers together in the dealership to enable the staff to communicate and collaborate with each other, and to share information and access resources.
2. A Dealer Access Network (DAN) connection to enable your dealership to access the Toyota applications e.g. SAP, Professor etc.
3. An internet connection to access the World Wide Web.
4. (Optional) If the dealership is a multi-franchise business then a Wide Area Network (WAN) connection to connect the dealerships together and share resources amongst the dealerships.

   All IT infrastructure devices should be UPS protected to minimize power failures and avoid data corruption.

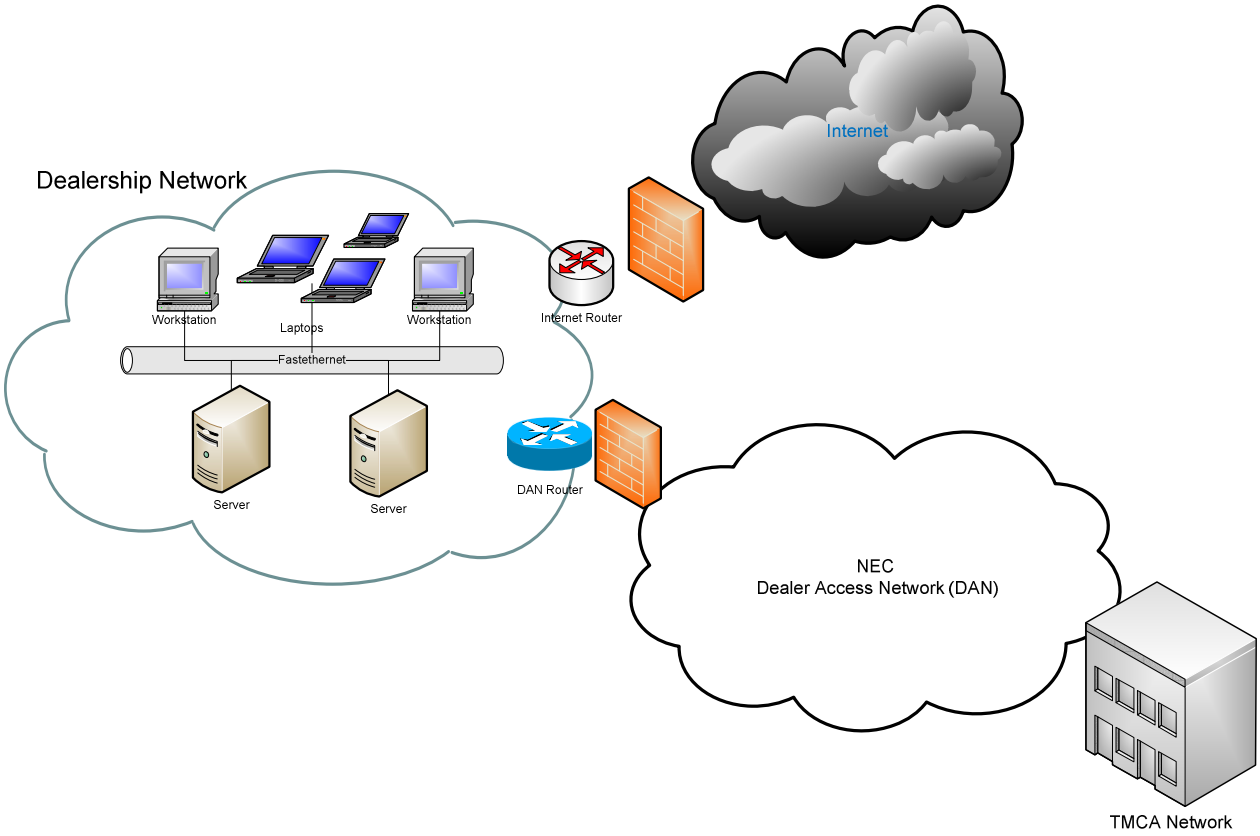

Figure 1 - Typical Dealership Network

2.4.2 LAN Guidelines and Considerations

Ethernet is the current standard for Local Area Networks today. It can connect workstations, servers and printers together at 10, 100 or 1000 Mbps (megabits per second) speeds. Ethernet technology requires a Network Interface Card (NIC) in each computing device. The card can be 10 Mbps (Ethernet), 10/100 Mbps (Fast Ethernet) or 1000 Mbps (Gigabit Ethernet). With a 10/100 Mbps NIC, depending on the LAN equipment being used, the device can operate at 10 or 100 Mbps. The 10 Mbps NIC is now becoming obsolete due to its lower speed and because 10/100 Mbps cards are available at almost the same price.

BEST PRACTICE

With increased demand for resource sharing within dealerships, the LAN standard has now been upgraded to 100 Mbps (Fast Ethernet) technology. Since the speed of a LAN segment is limited by the slowest component, it is highly recommended that 10 Mbps NIC's be phased out and replaced with faster 10/100 Mbps NICs. The higher LAN speed will enable faster transmission and exchange of information.

RECOMMENDATION

To future proof your investment, it is recommended to purchase 10/100/1000 Mbps (Gigabit Ethernet) NICs if replacing a faulty NIC. New laptops and PCs today are shipped with a 10/100/1000 Mbps NIC.

In addition to the NIC cards in the workstations, servers and printers, you also require LAN aggregation equipment to interconnect these devices. This LAN device is often referred to as a LAN Hub, LAN Switch or Hub/Switch.

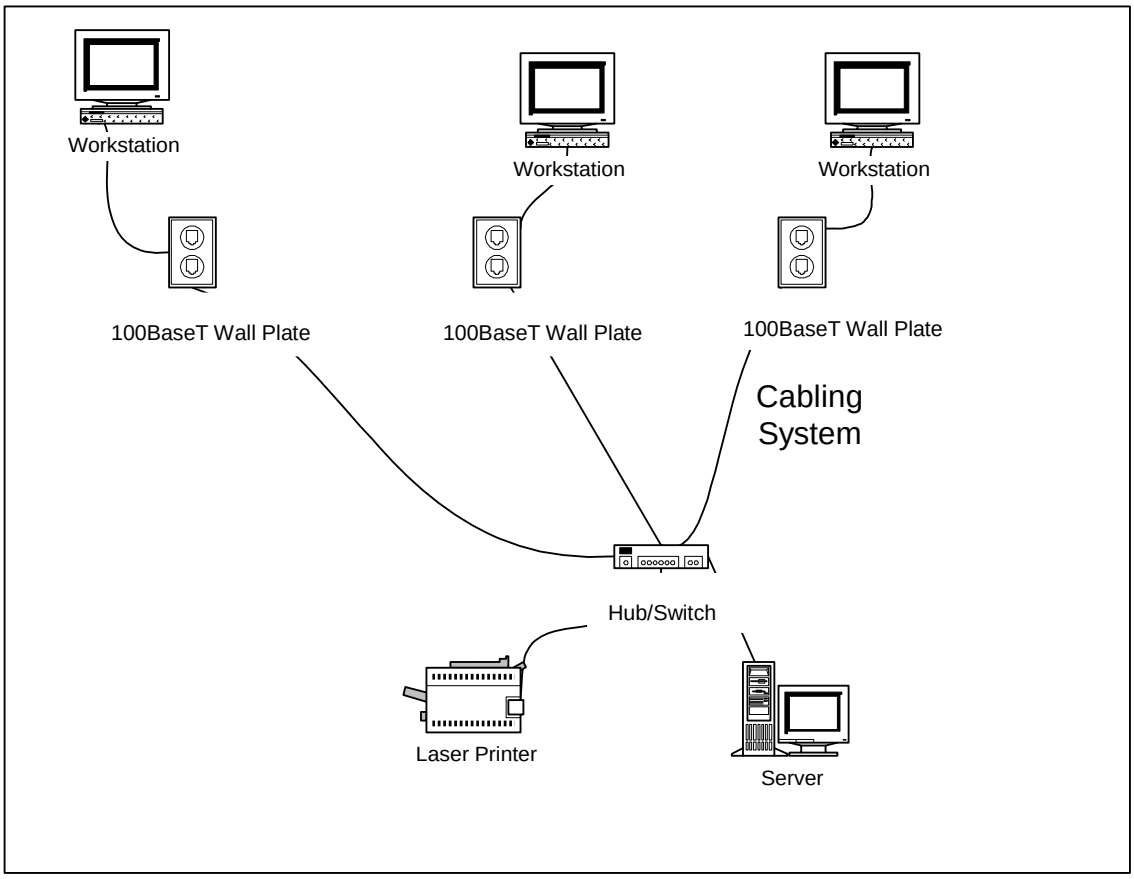

Figure 2 - Typical Local Area Network

A LAN is usually formed by connecting the NIC of each computing device to a distributed cabling system (usually via an RJ45 patch cable). The distributed cabling system provides network outlets in each office or work area (much like a electrical or telephone outlet) on one end for the computing devices to plug into, and a centralized termination point (the LAN Hub/Switch) on the other end. The LAN Hub/Switch provides the physical interconnection between the computing devices. LAN Hubs work using half duplex mechanism and are slower compared to LAN Switches they normally provide half the bandwidth.

The LAN design has great impact on the performance of the IT infrastructure. The services of a networking consultant should be availed to ensure the LAN is designed properly.

Since Hubs operate at half duplex, it is recommended that all Hubs be phased out and replaced with switches. LAN switches will enable faster transmission and full duplex communication.

RECOMMENDATION

To future proof your investment, it is recommended to purchase a LAN Switch if replacing a faulty LAN Hub or if extending your existing network. It is recommended to use a Cisco 2960 switch for connecting devices, there are multiple models of this switch series with different interface numbers, choose the right model depending on the number of users connecting to it.

Whilst some dealerships use Terminal Server across their environment, TMCA does not recommend the use of this technology unless in-house terminal server expertise is available and able to support the environment.

2.4.3 LAN Cabling Requirements and Considerations

Ethernet specifies the use of Category 5, 5e and 6 Unshielded Twisted Pair (CAT5, CAT5e and CAT6 UTP) cables as the physical media. This is a special 100-ohm unshielded cable consisting of four twisted pairs and is terminated with RJ45 connectors. This allows computing devices to be located as much as 90 meters (or 295 feet) from the Hub/Switch. To future proof your IT investment, Category 6 cables should be used in all new wiring implementations.

A qualified, certified contractor should be engaged to help design and install the distributed cabling system. The design should include considerations such as selecting an appropriate central location to enable proper termination of the cabling system and to house the hubs/switches, servers, WAN equipment etc. This central location should be selected/designed so that:

- All possible workstation connections will be within the design distance limits of Ethernet (i.e. within a radius of 90 meters).
- Workstations should have a dedicated port.
- Adequate electrical, air conditioning and other environmental requirements should be taken into consideration.
- Adequate space should be provided to facilitate easy servicing and maintenance.
- Appropriate security measures should be implemented to prevent unauthorized access into the area and tampering with networking or other shared resources.

The cabling system end points should be properly labelled, tested and documented. The dealership's wiring plan should be kept up to date.

2.4.4 Wireless Local Area Network (WLAN or Wi-Fi) Considerations

Instead of a wired LAN, a Wireless LAN (WLAN) solution can lower the LAN cabling costs and provide more connection flexibility to end-users, there are however, additional considerations to be taken into account, such as:

- *Cost*

  Each PC and server will need to have a wireless adapter card installed. One or more wireless access points (WAP's) are required which enables devices to remotely connect to an existing wired-Ethernet network. There are additional costs associated with surveying, planning, implementing and managing the wireless network and ensuring it is secure. Also consider installing firewall software on each PC on the WLAN as it can be vulnerable to outside penetration.

- *Current State of the Technology*

  WLAN technology is still evolving. There are multiple standards (e.g. IEEE 802.11a, 802.11b and 802.11g) that may not be compatible with one another. Secondly, there can be compatibility issues even when using products from different vendors that are based on the same Wi-Fi standard (e.g. 802.11n). There is no guarantee that the wireless investment will be protected should you desire to migrate to a newer technology.

- *Security*

  WLAN's are inherently insecure. In a LAN environment, access is restricted to the physical confines of the building structure. With wireless networks, access is possible to anyone within the range of the wireless signal. Physical security measures are not sufficient to ensure network security. Special efforts should be made, such as using WPA-PSK or WPA2-PSK private shared key authentication, data encryption, firewalls and MAC (Media Access Control) address filtering, including proprietary vendor security suite products, to reduce the vulnerability of the dealerships information assets from outside attacks.

- *Network performance*

  IEEE 802.11g is the most common Wi-Fi technology used in Australia. It has a theoretical maximum speed of 54 megabits per second but practically works at half. The 2.4 GHz frequency band it uses is shared by other radio devices such as cordless phones and microwave ovens. Depending on the environment, significant interference can occur, further reducing the network throughput. In comparison, depending on the network adapter card, your wired LAN will operate at 100 Mbps.

- *Wireless Internet Access for Customers*

  It is common these days to provide internet access to customers in cafeterias, airports, reception areas etc. while they wait for service. If your dealership intends to provide wireless internet access to customers, it should be ideally be on a separate internet connection to ensure they will not able to access the internal dealership network or the Toyota network. If you intend to share the existing internet connection, it must be properly firewalled and requires the services of a qualified network engineer.

- *Network Planning and Design*

  Without proper planning, design and installation, a WLAN can be disappointing. Determining user application, access and bandwidth requirements, choosing the appropriate technology and products, and completing a comprehensive site survey are important steps to ensure the success of the WLAN installation.

2.4.5 Dealer Access Network (DAN) Connection Requirements and Considerations

There are multiple DAN connection offerings from NEC; the speed of the link required by the dealership is dependent on the applications used, the size of the dealership, number of PCs at the dealership etc. For more information on the speed suited to your dealership environment, contact tSupport.

It is the dealership's responsibility to install a firewall to protect itself from any security threats from the DAN network.

2.4.6 Internet Connection Requirements and Considerations

There are numerous internet connection technologies available – dialup, cable, ADSL, SHDSL etc. The speed of the link is dependent on the applications used, the size of the dealership, number of PCs at the dealership, internet usage etc. Contact your local internet service provider for more information.

It is the dealership's responsibility to install a firewall to protect itself from any security threats from the internet and to safeguard against unauthorized access to the Dealer's business information and resources.
A router is required to share the Internet connection by multiple workstations. The router should support Network Address Translation (NAT) capability and at least static IP routing, although intelligent routing protocols such as RIP2, IGRP, and EIGRP are preferable

Normally in small to medium dealerships, the internet router is configured as the default gateway for workstations, servers and other devices; please ensure the router has routes to the following networks pointing towards the NEC DAN router:

192.168.108.0 /24

192.168.109.0 /24

10.9.100.0 /24

10.12.100.0 /24

As these routes are critical to the business continuity, it is advisable to undertake the services of a network consultant in configuring the internet router.

Medium to large dealerships may use static routes or run routing protocols in the internal dealership LAN. Any method can be used however, it is very important to ensure the routes given above are present in the routing tables of your site routers.

Depending on the importance of the internet connection to the dealership business comprehensive service level agreements should be worked out with the ISP (Internet Service Provider) or backup internet connection should be setup.

2.4.7 Firewall Requirements and Considerations

Whenever you connect to remote network, there is a possibility that unauthorized external parties (i.e. hackers) can gain access to your dealership's business information and resources. A firewall safeguards the dealership against such unauthorized access. As detailed in Figure 1, a firewall is critical to security of the dealership and more than one firewall should be deployed depending on the design of the network.

Selection of the desired Firewall solution is dependent on a number of considerations, including:

- Whether the Internet service is accessed via an analog dialup, cable, DSL, ISDN, wireless, satellite or leased line connection.
- The complexity of your local area network (LAN) environment; e.g. a multi-franchise environment where you may have other WAN connections.
- The firewall management and monitoring required. Regular monitoring of activity across the firewall will alert your dealership of any intrusion attempts so that steps can be taken to prevent illicit access. You should include such functions because failure to react to such intrusions could negate the effectiveness of your firewall. There are various levels of firewall management. Due to the complexity involved, it's normally best to engage the management services of your firewall vendor or ISP.

2.4.8 Managed Firewall service considerations

Without the proper know-how, implementing a firewall is of no use. Instead of implementing and monitoring the firewall yourself, a "Managed Firewall" service may be a better alternative.

- **Remote firewall configuration and management service**

With this solution, the 3rd party vendor provides a firewall on your premises. The vendor will help you define the security policies, configure the firewall according to your policies, and remotely monitor and maintain the firewall from its central office. The advantage of such a service is that you can defer the set-up, maintenance and monitoring of the firewall to the experts. You can leave it to them to alert you to any unauthorized attempts to access your IT environment.

2.4.9 Site Routers (Excluding DAN router)

If the dealership consists of multiple departments isolated on different segments/subnets, a router is required. It is not recommended to use PCs with multiple NIC cards

For small to medium sized dealerships, a Cisco 1800 series router should be installed for medium to large dealerships, a Cisco 2800 series router is recommended.

2.4.10 IP Addressing

All network devices require an IP address to function; depending on the size of your dealership the IP address assignment can be done automatically via a DHCP (Dynamic Host Configuration Protocol) Server or can be assigned statically to each device. Using a DHCP server means if a new PC joins the network, it can automatically get an IP address can start using the network, if not the PC will not be useable unless it has been assigned an IP address manually.

If the site has a Cisco router than it can configured to provide IP addresses automatically.

2.4.11 Domain Name Server (DNS)

Depending on the dealership size, one of the two possible configurations for dealership DNS must be used to optimize both the dealership and Toyota DAN network experience.

2.4.11.1 Option 1: Forwarding

If a dealership has less than 20 seats (workstations), it is considered reasonable to forward all DNS traffic to Toyota via the DAN Network to enable resolution for toyota.com.au and tmca.com.au as this will not create a significant load to the DAN network nor Toyota DNS Servers in doing so.

To achieve this, either at the workstation or your local router end, configure both Toyota DNS Servers:

1. 192.168.109.38 – Primary
2. 192.168.109.138 – Secondary

2.4.11.2 Option 2: Zone-Transfer

If your dealership is in the category of having more than 20 seats (workstations), a dealership must provide a local DNS Server either Microsoft Windows Server or Linux to transfer the DNS Zone information locally where it can be queried without causing excessive overhead via the DAN network. The picture below depicts this configuration.

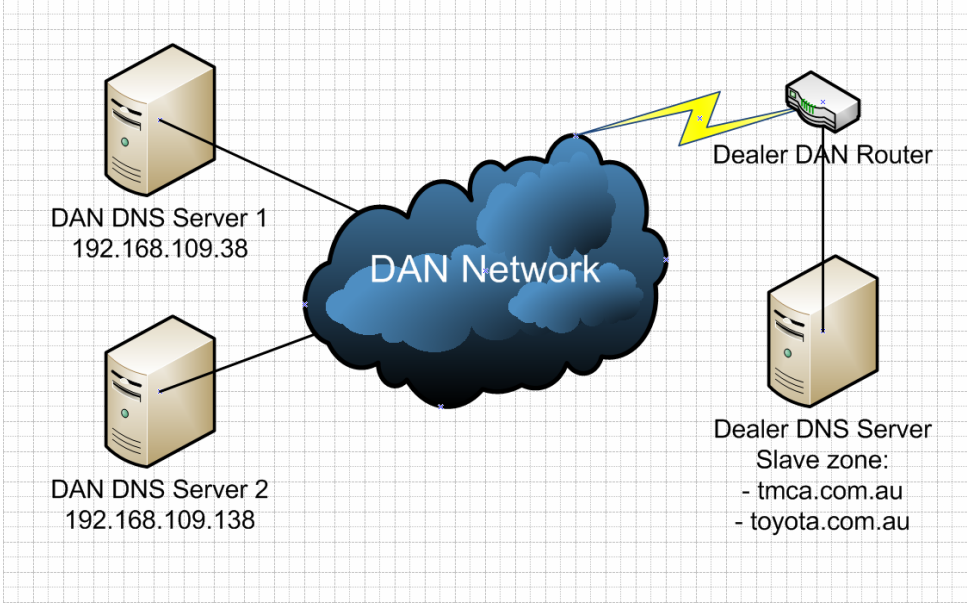

Figure 3 – Zone Transfer DNS Configuration

To achieve this, configure the Dealer DNS Server with two slave zones: tmca.com.au and toyota.com.au with the server IP Addresses as depicted in the diagram above. The zones should only be transferred every 24 hours.

2.4.12 Network Diagram

You should maintain an up-to-date Network Diagram of your IT environment because an accurate Network Diagram will facilitate asset and network performance management as well as problem diagnosis and resolution. As your IT staff and/or Technology Partner is implementing your dealership local and wide area networks (LAN/WAN) and cabling system, insist that a detailed network diagram be produced as part of the exercise. The network diagram should include:

- A detailed diagram of the Local Area Network as implemented, and the design criteria (e.g. dedicated LAN segments for each server, Service Reception, and Service Bays to facilitate good network performance, shared LAN segments in the rest of dealership, etc.).
- Identification of each server, workstation and printer, and how it is logically connected to the LAN segments. The identification should include workstation name and/or serial

number, assigned network address and a physical locator (e.g. office description or location).

- How the ISP connections (primary and backup) and other WAN links are connected to the dealership LAN. The firewall/gateway type and identification, ISP name, service type, link speed and client ID must be clearly documented.
- A separate cabling systems diagram outlining cabling drops or outlets in the dealership, how these are being identified or labeled, location of the wiring closet(s), and how each cable run is terminated in the wiring closet(s).

As changes are made to the network (e.g. adding new workstations or relocating an existing workstation), make sure that the network diagram is updated immediately and accurately.

2.5 Support Requirements and Guidelines

2.5.1 Support Requirements

In order to protect your IT investment, you need to have in place an effective IT support infrastructure.

Although TMCA provides training and support for its applications and services as will your DMS vendor for your DMS system, you still need to have resources to manage and support your own IT environment. This includes installing, upgrading and maintaining your

- servers and workstations (and their associated hardware and software)
- printers
- local and wide area network equipment and facilities, including the ISP connection(s).

Your IT management process should also include enrolment and administration of users on the TMCA applications.

Depending on your requirements and circumstance, your IT support infrastructure can be comprised entirely of in-house resources or it can be a combination of your in-house resources complemented by expertise from a technology partner.

In the absence of in-house technical resources, it is imperative that each dealer contracts the services of a local technology partner.

2.5.2 Dealer Technology Administrator Role and Responsibilities

The Dealer Technology Administrator is a key resource for your dealership. You need to appoint an administrator (with proper backup) to manage and co-ordinate all IT-related activities in your dealership. The Dealer Technology Administrator should be the first line of support within your dealership, and the main interface with tSupport, the TMCA dealer technology support centre to resolve usage problems with TMCA applications.

The Dealer Technology Administrator is also responsible for the management of all TMCA application (e.g. DRIP) user ids in your dealership via the TMCA Delegated Administration application. When enrolling new users, he/she should ensure that the correct job functions and access authorities are established. As employees leave your dealership, their user ids should be deleted immediately to prevent security exposures.

The Dealer Technology Administrator should also keep track of all the workstations in your dealership; when they were acquired, where they are deployed, and when they are expected to be replaced. It is also very important to keep track of all the software licenses and associated keys, as well as all the Windows install and recovery disks.

So that the Dealer Technology Administrator can function effectively with the right level of authority and accountability, we recommend that he/she report to the General Manager or Controller.

More details about this role are in Section 7 - Role of the Dealer Technology Administrator.

2.5.3 e-Mail Administrator Role and Responsibilities

BEST PRACTICE

You should have an e-Mail administrator to manage all your e-mail accounts. The job function includes:

- Setting up new e-mail accounts and ids.
- Changing passwords immediately and monitoring incoming mail of e-mail accounts when the associated employees are no longer with the dealership.
- Ensuring that appropriate etiquette is being followed in all external e-mail communications.

The e-Mail Administrator does not need to have in-depth IT skills. However, he/she should be familiar with the e-mail applications used in your dealership, especially if several employees are sharing a common workstation for their e-mail accounts. The e-Mail Administrator function can be performed by the Dealer Technology Administrator, or can be assigned to somebody else in the dealership.

2.5.4 Technical Support Role and Responsibilities

You also need in-depth IT skills and knowledge available either from within your dealership or from a technology partner. Technical support can help you perform regular maintenance on your IT equipment, keep your IT environment operational and resolve any problems you may have in your IT infrastructure.

When you engage a technology partner, make sure that they will be able to, and are contractually required to, provide the service level that meets your business needs; e.g. be able to provide on-site support within the same business day. Refer to the Technology Partner Selection Guide (section 6) for more information on qualifying potential technology partners.

2.5.5 Skills Requirements Summary

The following table summaries the skills required for your dealership:

	Area of Responsibility	Dealer Technology Administrator	Technical Support	End-User
Systems	Windows	3	5	2
	Web Browser	2	5	2
	Adobe Acrobat	2	4	2
Network	Local Area Network	3	5	
	Internet Connection	3	5	
	Firewall/Gateway	2	5	
	Anti-Virus	3	5	2
MS Applications	MS Word	3	5	2
	MS Excel	3	5	2
TMCA Applications		3	4	2
DMS		3	4	2

Table 2 - Staff Skills List

1= Understand but need help to configure or use
2= Understand and can configure or use
3= Able to help others configure or use
4= Can define problem and work with tech partner or TMCA to resolve
5= Can trouble shoot and resolve most problems

2.5.6 Skills and Training Considerations

Without doubt, the more IT literate your staff is, the higher the dividend on your IT investments.

Your staff should be given the opportunity for basic computer training such as Microsoft Windows, Internet browser, Microsoft Word or Excel, from your technology partner, or by attending classes offered in your community.

In terms of TMCA applications, TMCA's tSupport offers support for TMCA applications while your DMS vendor provides training and support for the DMS applications.

Your dealership's Technology Administrator is responsible for providing first level day-to-day operations support within your dealership and to serve as the main interface to TMCA in all IT-related matters.

Your Dealer Technology Administrator should be a professional with reasonable overall IT training and experience. She/he should have good leadership and communications skills to help your staff use and leverage your IT infrastructure to perform their specific jobs. Ideally, your Dealer Technology Administrator should be an on-going learner with the initiative to pick up new skills and proactively seek out better ways of doing things.

You should *also* encourage your staff, especially those who interface directly with customers, to routinely use their workstations to develop more proficient computer skills. Your sales and service representatives should be using the Internet to research the competition, and use e-mail to communicate with their customers.

***However, to* prevent abuse of privileges, you should *also* spell out a computer and Internet usage policy, including what is appropriate and inappropriate use of the staff's time and IT resources. Section 4 provides a sample computer and Internet usage policy that you may tailor according to your dealership's needs.**

2.6 Business Continuity and Security Requirements and Considerations

2.6.1 Preventive and Reactive Measures

As you rely more and more on your IT infrastructure to support (run the business), enable (grow the business) and drive business changes (transform the business), the availability, reliability and security of your IT resources becomes more and more critical.

There are measures you can take to prevent or reduce exposure and mishaps in your IT environment. However, despite best practices, outages do occur. You must also have measures and processes in place to enable you to recover from outages and disasters without serious interruptions to the business.

2.6.2 Preventive Measures

The preventive measures to take should include the following:

- Computer virus prevention and control
- Blocking external intrusion
- Regular housekeeping
- Protection from physical and environmental elements.
- Password management

2.6.2.1 Virus Prevention and Control

As you probably know, computer viruses arrive all too frequently these days. In serious situations, computer viruses can destroy all the data files in your computers, and/or render your computers useless. New strands of virus are being created everyday. The paranoia is understandable but you should also realize that infection from computer viruses could be easily avoided if appropriate precautions are taken.

Computer viruses can get into our systems most commonly through

- e-mail
- downloading files from the Internet which contain a virus
- *Internet relay chat (IRC) and file-sharing networks, such as LimeWire.*
- opening an infected file stored on a USB disk or CD given to us by a friend or colleague.

Presently, you cannot be infected by a virus by just reading an e-mail message, unless you open an attachment with a malicious code in it. However, new forms of viruses and ways of transmission are constantly being developed and caution must be exercised at all times.

The following are some "do's" and "don'ts" that can help you *reduce* your exposure to computer viruses *and external intrusions*:

- Make sure that you have an anti-virus program installed and active in every server and workstation in the dealership. The anti-virus programs must be updated regularly, at least once every week. These programs use a database to recognise the viruses. This database must be updated when new viruses are discovered. You can get the updates by subscribing to a Live Update service from the anti-virus program vendor (e.g. Symantec or McAfee).
- *Always keep your operating system (Windows), Internet Explorer and Anti-Virus program patch levels up-to-date. Consider within your environment for appropriateness to subscribe to automatic update download, or live update services, and install patches and/or critical updates when they become available. Update your Anti-Virus database often to recognise the latest threats.*
- ***Never*** open an attachment from an e-mail message if you do not know the Sender, *or expect file attachments from the sender*. Be especially suspicious of files with extensions (last 3 characters) of .PIF, .BAT, .COM, .EXE, VBS *or .SRC*, even if it is from somebody you know. Some viruses, once they get into your friend's system, can start propagating themselves by sending infected messages automatically to everybody in the address book. If you are not certain, detach the file and scan it with your Anti-Virus Program prior to launching it.
- *If you have your own e-mail server, configure it to block or remove e-mail that contains the attachments that are commonly used to spread viruses, such as .VBS, .BAT, .EXE, .PIF and .SRC files. The e-mail server should be connected to an external safe area (commonly known as a Demilitarized Zone or DMZ) and never directly to your dealership's internal LAN. Many e-mail servers have known vulnerabilities that can be exploited by intruders to gain access to that server, and hence access to the rest of your network.*
- *The same goes for your dealership's web servers. Your web servers, if hosted at your premise, must be connected to the DMZ and never directly to your dealership's internal LAN.*
- *Take regular inventory of all software used in all the computers in your dealership. Remove all unused, unneeded or unauthorized software from the systems.*
- *Don't download files or software from the Internet unless you know it is from a trusted source. Don't execute software downloaded from the Internet until it has been scanned for virus. Some websites may also download tracking software (commonly known as "Spyware"), without your knowledge or consent, into your workstations. Not all Spyware are malicious, but some can be very nasty. They can send information on activities in your workstation to a remote location using your Internet connection.*
- *Schedule automatic regular full system scan on users' PC's at least once every month to check for viruses and deception software (e.g. spyware) and remove them if discovered.*
- *Keep your Internet Explorer security setting to medium or high (under "Tools", "internet Options", "Security", "Custom Level") to prevent Web sites from downloading software without permission.*

- *Don't install non-business related and unauthorized software (e.g. Limewire) in your workstations. They use up storage space and cycles on your workstations, and can be sources for spyware.*
- Use the Anti-virus Program to scan USB disks or CDs that somebody else gives you prior to opening or saving any files on your computer.
- Schedule the Anti-virus Program to automatically perform regular scans on all your hard drives. Fix any problems it may detect.
- *All PCs connected to your dealership's LAN should have their analog modems disconnected. If they must be used, they should only be used for making outgoing calls. Auto-answer should be disabled.*

If you suspect that you have been infected with a virus (e.g. your PC does not boot from hard disk, or freezes after booting, or frequently crashes without reason), you can follow the following steps to try to recover:

1. *Turn off the PC immediately.*
2. *Isolate or detach the PC from your LAN to prevent further damage.*
3. *Boot from the Recovery Disk*
4. *Run the Anti-Virus Program to scan your hard drives.*
5. *Repair or delete any files that the Anti-Virus Program suspects contain a virus. You may be able to download removal tools from the Symantec or McAfee websites to help you restore your PC.*
6. *Scan your hard drives again.*
7. *Scan all floppy disks or CDs containing your backup files. Make sure they are clean before you try to recover any of your lost files.*
8. *Try to identify the infection source and isolate it so that it cannot damage your system again*.

2.6.2.2 Blocking External Intrusion

The Firewall/Gateway that you install with your ISP Connection Solution will not only enable all the workstations on your dealership local area network (LAN) to share the Internet access line, it will also *help guard against* outside intrusion *and potentially harmful contents on the Internet*. Your Firewall/Gateway should be set up with *the help of a qualified network expert and include the following security policy considerations:*

- **Permit all workstations on your LAN to access the Internet but deny ALL access from the Internet into your network.**
- **For outbound traffic, set up Network Address Translations (NAT) to utilize external Internet IP Addresses but deny ALL Inbound NAT's.**

This will *help* prevent hackers from gaining access to your servers and workstations so that they cannot steal or destroy your information assets, vandalize your systems, or use them to launch illegal activities, such as denial of service attacks. Regular monitoring of activity across the firewall will alert your dealership of any intrusion attempts so that step can be taken to prevent illicit access.

Be very careful with deploying **wireless technologies** in your networking environment because they can be potential security hazards. Current IEEE 802.11 standards and wireless protocols (e.g. Wired Equivalent Privacy or WEP) have inherent security weaknesses. With scanning and GPS (global position system) devices readily available, intruders can easily detect and pinpoint the location of Wireless Access Points (WAPs). If you have a Wireless LAN (WLAN or Wi-Fi) in your dealership, unless strong security measures are taken, an eavesdropper can intercept and decipher traffic flow within your network, including e-mail, browsing, file transfers, user ids and passwords, and thereby gain access to your systems and information assets. Worse yet, because hardware is now readily available in the market place to enable users to set up their own Wireless Access Points, your efforts to set up perimeter security control (e.g. firewall/gateway) can be easily

BEST PRACTICE

bypassed. Policies should be spelled out and steps taken to prevent the establishment of unauthorized WAPs (commonly referred to as “Rogue Wireless Access Points) within your networking environment.

2.6.2.3 Housekeeping

To keep your computer systems in top shape, and to reduce chances of new security exposures, your Dealer Technology Administrator and staff need to perform house-cleaning duties regularly.

As you visit Internet Web sites, the browser program accumulates temporary cache files, Internet cookies, plug-in programs, and various control files. Many of these files are used only once but remain on your hard drive. As you use your PC, you may also produce many redundant files, obsolete files (e.g. deleted files in your Recycle Bin), and programs you no longer require. The unnecessary files need to be cleaned out from time to time; otherwise, sooner or later, the hard-disk space on your computers will get clogged up.

BEST PRACTICE

You can manually erase them (e.g. selecting and deleting all files with a .tmp extension), use the Disk Cleanup utility program under System Tools in your Windows Accessories, or you can install and use a house cleaning utility program, such as Norton Clean Sweep.

BEST PRACTICE

As information is written on the hard disk, it may be fragmented to fit into whatever space is available. Extensive fragmentation can impact the performance of your workstation**. It is advisable for users to run the Disk Defragmenter utility program under System Tools in your Windows Accessories, or use a utility program, such as Norton Utilities, at least once every month, to consolidate and optimize the hard-disk space on their workstations.**

Computer programs are far from perfect, including operating systems, such as Windows. As new bugs or holes are discovered (sometimes unfortunately by hackers) and fixed, updates and patches become available. These patches should be applied by the Dealer Technology Administrator.

Another important reason is user administration. As an authorized Toyota dealer, you can gain a competitive edge from timely access to up-to-date information, such as the price guide, technical bulletins, diagnostic information, incentive programs, etc. It is imperative that only authorized users within your dealership are given the rights to access such privileged information. Even at that, each user should only be able to access applications and data to which they are entitled. For example, you would likely not want all the financial information or dealer costs to be common knowledge within the dealership. TMCA is empowering each dealer to decide how it wants to authorize information access within its own dealership through the Delegated Administration application.

With the Delegated Administration application, your Dealer Technology Administrator, based on instructions from you, the dealership management, have to register and authorize each user in your dealership. During enrolment, the Dealer Technology Administrator will need to specify for each user which TMCA applications he/she is entitled to access. It is your responsibility to ensure that the user records are kept up-to-date and that the access rights are not abused. TMCA is entrusting you with the administration of users within your own dealership so that your staff can leverage information and tools to their best advantage.

BEST PRACTICE

Nevertheless, it is in your best interest, as well as ours, to safeguard these valuable information assets and you must tell us if there has been any unauthorised access to, or use of, our information assets. You and your Dealer Technology Administrator must be careful in granting access rights. Upon departure of former employees, the Dealer Technology Administrator should immediately delete their user ids using the Delegated Administration application. This will reduce the chance of security exposure.

From time to time, TMCA will conduct security audits to ensure that the user records submitted to the Delegated Administration application reflect the actual status of your employees.

BEST PRACTICE

Each user must also perform regular housekeeping on their e-mail accounts. It is all too easy to leave obsolete and useless e-mail messages in in-baskets and folders. If excessive obsolete e-mail messages are kept on the server, they will impact the server’s

storage utilization and performance. If they are stored or downloaded to the user workstations, they will use up storage space and eventually the workstations' ability to receive mail. Make it a habit to delete or archive obsolete messages regularly.

When an employee leaves your dealership, your e-Mail Administrator must change the employee's e-mail passwords immediately and monitor his/her incoming mail. This is to prevent the departed employee from using your dealership's name to communicate with your customers or other parties under false pretence. However, it is usually not a good idea to delete the e-mail account immediately because you may require some of the employee's e-mail or folders later on, or you may want to continue on-going communications that the departed employee may have with some of your customers. To ease the monitoring effort, it is a good practice to set up message rules in the former employee's id to automatically forward any new incoming e-mail to the accounts of associates who are taking over the responsibilities. Eventually, the e-Mail Administrator should delete the obsolete e-mail accounts.

2.6.2.4 Protection against Physical and Environmental Elements

You should have qualified electricians install the dedicated electrical circuits that provide power to your computer equipment. Plugging computer equipment to extension cords can sometimes create a grounding problem. It is recommended that all computer equipment be plugged directly into wall outlets with proper grounding. To prevent overloading, any devices sharing an electrical circuit must not cause total amperage to exceed 80% of the circuit's amperage rating.

You should consider installing a surge protector at the main circuit breaker to safeguard against sudden high voltage electrical power surges (e.g. caused by lightning) destroying your electronics equipment.

Each laser printer should also be on its own dedicated electrical circuit. It has been found that surges in some laser printers can damage other electronic equipment connected to the same circuit.

If you do not want sudden electrical power outages to impact your servers, you should consider including an Uninterruptible Power Supply (UPS) in the server configurations. An UPS provides power to the servers for the time required to restore primary power. If power cannot be restored, UPS will systematically shut down the servers to ensure that the systems are closed properly and reduce the risk of data loss. Both the ERA2 and Sales Vision servers come equipped with UPS.

2.6.2.5 Password Management

All desktops and servers must be password-protected to ensure no unauthorised access to dealership and TMCA data.

In addition, users should be provided with advice on proper password management such as:

- No sharing of computer accounts and passwords
- Do not tell a password to anyone
- Do not write down a password
- Do not communicate a password by telephone, e-mail or instant messaging
- Be careful to log off before leaving a computer unattended
- Change passwords whenever there is suspicion they may have been compromised
- Passwords should be alpha-numeric with a minimum length of 8 characters.
- Please ensure all factory default passwords on IT devices are changed upon installation.
- Passwords should be unique and not easily guessed (e.g. Avoid common words or easily identifiable passwords like Dealer123).

2.6.3 Reactive Measures

Despite the best planning and precautions, outages do occur. You must have measures and processes in place to prepare and enable you to recover from outages and disasters without serious interruptions to the business.

The following are some reactive measures that you should include:

- Computer emergency response
- Data backup and recovery
- Backup for the ISP connection.

You must test and document the reactive measures and processes. Trying them out for the first time during a disaster is no guarantee that you will have business continuity. You should go through "fire drills" to ensure that the recovery processes work.

2.6.3.1 Computer Emergency Response

Computer emergencies will occur. For example, your computers may be under a serious virus attack; the ISP connection may be down for an extended period of time; the hard drive in a server may have crashed.

You must have a computer emergency response process in place to handle crisis situations. The process should include a definition of roles and responsibilities. For example, how do you decide what actions to take? Who is in charge and making the decisions? Who monitors? When and how should you return to normal operation?

As in all emergency situations, the most important thing is not to panic. **The following is a checklist of questions that you, your Dealer Technology Administrator and technical support should consider prior to taking any actions:**

- What seems to be the problem? Can we describe the symptoms?
- Are there any steps we can take immediately to stop the situation from getting worse? For example, if one or more computers are under a virus attack, it may be advisable to shut down the LAN and all other computers before the situation spreads.
- What recent changes have we made to our IT environment? Could this be the cause?
- What seems to be the root cause? Can it be isolated so that the problem won't recur when we apply the recovery process? For example, if a computer virus is destroying all your data files, before you try to restore with backup files, isolate or clean out the virus first.
- Do we have enough expertise to fix the problem? Do we know what we are doing? Can we leverage support from the IT vendor as they are often best equipped to remedy the fault or failure quickly and effectively?
- What are the alternatives to fix the problem? Why is the recommended approach better than the others?
- Can we back out the "fix" if this does not seem to alleviate the problem?

All too often in emergency situations, people adopt 'corrective measures' that only exacerbate the original problem. It is advisable to always think first; then do one thing at a time. If the action does not resolve the problem, back out the change and try something else. By backing out, you will always return to a common base and prevent a "snow balling" effect.

If the fix is a temporary measure (e.g. you use a dialup line to bypass the downed ISP connection), include a process to return to normal operation. However, before you do, always make sure that the root cause has already been addressed.

It is advisable to do a post mortem after an emergency situation to understand and prevent the circumstances that caused the problem from recurring.

2.6.3.2 Data Backup and Recovery

You must have a process to backup and restore critical business data, including financial information, and e-mail ids and databases on your servers and workstations. This is to ensure that your business will not be seriously impacted if the data files are damaged, accidentally or maliciously.

You should backup files on auxiliary devices, such as tapes or CDs, if possible. This will give you the most flexibility for recovery, including from an off-site location, if necessary. Your backup process should include careful labelling and storage of backed up information. Test your restoration process to ensure that it works.

A backup cycle should be defined and followed using multiple labelled auxiliary media, such as tapes or CDs/DVDs. For example, consider having separate media for:

1) Nightly back ups – Can be run to include full data back ups or only capture incremental changes that occurred that day

2) Weekly backups - Regardless of the number of full backups you create during the week, the LAST full backup of the week is considered the WEEKLY backup.

3) Monthly back ups - a Full data back up should be conducted at the end of every month and stored off site.

4) Yearly back ups – should be completed to be able to go back to a point in time for legal and financial reasons. This should also be stored off-site.

Rewriteable media (e.g. tapes, read/write DVDs) can be rotated through the nightly and weekly cycle of back ups avoiding excessive media costs. You can reuse (recycle) the DAILY and WEEKLY backup tapes or take them off site for permanent storage.

2.6.4 Network Backup Requirements and Considerations

If you use a high-speed ISP connection (e.g. ADSL or Cable), choose a firewall/gateway solution that can support an analog dialup connection as a backup. The dialup connection will ensure business continuity (e.g. enable you to order parts and manage sales leads) if the high-speed access service has an extended outage. *This is the minimum backup requirement.* You may choose more robust backup solutions – e.g. use a residential-grade cable service as a backup to the primary DSL connection. When you are on a slower backup ISP connection, you may want to limit the access to more critical business functions until normal service is restored.

If you use an analog dialup as your main Internet access, subscribe to service from another ISP as backup, so that you can dial into it if your primary ISP has an extended outage problem.

2.7 Green IT Guidelines

TMCA's Green IT Policy was launched in August 2008 and is aimed at minimising the environmental impact of TMCA's information technology (IT) assets and facilities. This policy focuses on three key areas which outlines ISD's commitment in addressing the following areas:

1) Managing equipment disposal
2) Optimising infrastructure
3) Managing energy usage

As a result of this policy, a number of initiatives are now taking place within TMCA to:

1) Reduce our carbon green house gas emissions (CO2) by installing energy saving features on our computers and printers
2) Improve our equipment optimisation by consolidating various systems onto single hardware platforms
3) Address the lifecycle management of our equipment from purchase through to eventual disposal

4) Reduce paper wastage by implementing paper saving features on our printers

Green IT has a heavy focus in TMCA as we strive for the number 1 reputation in environmental leadership in line with the President's Goals.

Here are some guidelines to implement a Green IT policy at your dealership. Implementing these initiatives can equate to a cost saving as you will be using less power and/or paper.

2.7.1 Printing

- Recycle all office paper or at the very least dispose of office paper into a recycling bin
- If your printer is able to do this, implement double sided printing (called Duplex)
- If you printer is able to do this, set it to go into energy saving mode after 10 minutes of inactivity
- Investigate to see if there is a way to recycle your printer toners - this may require a call to the manufacturer
- Use the Print Preview function before printing a document to avoid having an extra line of text printing on a page by itself
- Attempt to minimise printed handouts at meetings as staff will usually end up disposing of them anyway. Alternatively, consider using a video projector to display required content at meetings

2.7.2 Computers – Energy Saving and Disposal

- Be sure to turn all computers and monitors off at the end of the day
- Unplug any device that is not likely to be used for a period of time
- When disposing of IT equipment, consider using an environmentally friendly disposal company rather than just throwing them out
- Consider setting your computers to go into energy saving mode when not in use. To do this, go to Start, Settings, Control Panel, Power Options. Set your Monitor and Hard Disks to turn off after 10 minutes. Once a computer is in this mode, it will "wake up" within 2 seconds of activation

2.8 Wrap-up Comments

This Dealership IT Guide is designed to help you plan, budget, install and manage a sustainable IT environment. By following the recommendations and considerations, you should realise a reasonable return on your IT investment.

In addition to servers and workstations, your local area network and ISP connection should be part of your IT infrastructure. Your Dealer Technology Administrator is a critical resource to co-ordinate and manage your IT assets. Make sure that you staff this position with the right skills and qualifications.

Training your people to become more proficient and literate with computers can pay handsome dividends as well because they will make *fewer* mistakes and learn to leverage technology to perform their jobs better.

This Guide is a living document. As new business initiatives are introduced, or new beneficial technologies become commonly available, we will be publishing updates to this document.

3 Business Applications

3.1 The Evolving Business Environment

The Internet is changing the way we learn, shop, play, invest, communicate and do business in a very significant way. Without exception, it is also driving a revolution in the automotive industry. For example, in Australia, more than 74% of people looking to buy a new car are already using the Internet for research before they purchase their vehicles. This trend is *increasing* as the more computer and Internet literate Generation "X" and "Y" population join the consumer mainstream.

e-Business is a term that is commonly used to refer to the transformation of key business processes through the use of Internet technologies. e-Business can be directed business-to-consumer (B2C), business-to-business (B2B), or business-to-employees or enterprise (B2E).

Through easy-to-use technologies, such as the Web Browser, and the reach and range of the omnipresent Internet, automotive manufacturers and their dealers can reach and market to a significantly larger customer base. Through rapid information access, aggregation and customisation, operations and communications between the manufacturer and dealers, and between dealers and customers, can become more effective and efficient.

The shakedown of dot-com companies *in 2002/2003* is just part of the evolution of the e-Business model. What is emerging today is the integration of e-Business into the existing business fabrics. Instead of having distinct e-Business units, enterprises are now integrating IT and e-Business thinking and practices into existing business strategies and processes. The modern successful enterprises are the ones that know how to deploy e-Business and information technologies innovatively and effectively to enhance competitiveness and market position.

3.2 TMCA's e-Business Strategy

TMCA is a leader in leveraging information and e-Business technologies to improve operational efficiencies and market share. Since 2002, TMCA has been steadily introducing industry-leading initiatives in the B2C, B2B and B2E arenas. There are three main objectives that the TMCA e-Business strategy focuses on:

- **Enhance TMCA-Dealer Relationship:** Build on the already strong relationship with our dealers by helping them to enhance their franchise values. This means working and collaborating with our dealers to:
  - improve their efficiencies and capacities
  - achieve our common business goals
  - strengthen Toyota's brand image
  - serve customers better through information sharing and consolidated relationship management over the customer life cycle.
- **Enhance Customer Relationship:** Expand our loyal customer base by becoming more customer-centric, and making it easy for customers to do business, and to want to do business, with our dealers. We want to make them feel special as Toyota customers. We also want to make it easy for our dealers to market vehicles and services to new and existing customers. We can realize these objectives by making our product information more readily available. This will enable our:
  - customers to easily and objectively comparison shop
  - dealers to focus on customer relationship management in every phase of the customer life cycle.
- **Enhance Core Competency:** Enhance TMCA and its dealers' core competency as an integrated vehicle marketing, distribution and servicing organization. This means introducing and integrating e-Business and information technologies and initiatives into

business processes, in areas where the e-channel can improve their efficiencies, effectiveness, capacity and capabilities, compared to using existing traditional means. The objectives are to enable TMCA and its dealers to

- lower the costs of doing business
- profitably grow the business.

3.3 TMCA's Business Applications

The following is a brief description of the major TMCA business applications used by dealerships:

- **SAP DANV**

  This is a SAP-based system used by dealers to order vehicles, search and swap stock, COSI and RDR.

- **SAP Winpaq**

  This is a SAP-based TMCA Warranty system, for campaigns and processing of warranty claims.

- **CORE/mainframe**

  This is a mainframe-based parts ordering system.

- **TDOS**

  This provides the ability to order parts for stock as well as providing an upload file for dealer's DMS systems.

- **DSR (Dealer Sales Reporting)**

  This is sales reporting for Service & Parts. This is a daily download from the Dealer's DMS to TMCA containing service and parts sales information. The KPI comparison based reports are created in return for dealers to use.

- **TIPS**

  This is the Dealer financial reporting / management information system. Used for dealers to provide TMCA with monthly financial, sales, and other information.

- **SARIS (Service and Repair Information Service)**

  This is a web-based service and repair information system.

- **DRIP (Dealer Regional Intranet Portal)**

  This is an information site for dealers including bulletins, pricing etc.

- **Toyota Central**

  This is an Internet site for Sales Society and general sales information.

- **The Professor**

  This is an in-dealership product knowledge system. It explains product features and Toyota technology using short video clips, diagrams, photographs, and PDFs. It can be used as a point of sale device and as an in-dealership sales training tool.

- **Vehicle Inventory Update (Barossa) & Vehicle Invoicing (Uluru)**

  Data streams from TMCA to dealers' DMS system containing real time information regarding vehicle supply status, inventory, dealer ETA (Barossa) and wholesale invoice advice (Uluru).

- **PAPIS (Product and Pricing Information System)**

  Data streams from TMCA to dealers' DMS system containing real-time information regarding vehicle specification, retail pricing, fleet pricing and accessory fitment information.

- **Showroom Direct**

  This is a TMCA Showroom system for dealers.

- **Customer Order Web Tracking (COWT)**

  This is a web-based service for customers to track the arrival of their ordered vehicles.

- **Marketing Extranet**

  Web based site for Vehicle and Accessory marketing and brochure materials.

- **TFS**

  Toyota Finance Systems such as Atlas

- **Dealer Score Card**

  This is a set of reports showing sales and customer satisfaction results

- **My Fleet**

  This allows authorised people in the dealership to access Fleet Price lists

- **Network Central**

  This maintains information about the dealership and the staff working at the dealership

- **TUNE**

  TMCA's evolutionary Dealer Management System to support Dealer Operational Process improvements to reduce waste and enhance customer value.

4 Sample Computer and Internet Use Policy

The dealership management should establish a policy to advise associates on appropriate and inappropriate use of the dealership's computer and networking facilities. Dealership staff are required to read, accept and comply with the policy if they expect to use the facilities. This could be done via a click through agreement each time the employee logs onto the system; or the dealership could give a copy of the policy to each employee for them to sign and include a statement that each time the employee logs onto the system, this constitutes acceptance of the policy.

The policy should include a statement that employees should not have any expectation of privacy in respect of their internet usage, making them aware that usage will be monitored.

The following is a sample policy that you may customise for your dealership:

DO	**Employees are encouraged to use the dealership's computer and Internet access facilities:** 1. For business related activities to enhance our productivity, efficiency and profitability. This includes: • Accessing and leveraging the TMCA applications and services. • Accessing the dealership management applications, • Adapting and streamlining TMCA initiatives into the dealership business processes. 2. To enhance the dealership's competitiveness. This includes: • Researching competitive information on the Internet, including visiting OEM, other dealership and auto broker websites. • Using e-mail to communicate with customers. 3. To enhance professional skills and become more proficient with information technology and the Internet so that you can use the new tools more effectively. This includes: • Using on-line tutorial and help facilities to acquire better computer and application skills, such as Microsoft Office and the Web browser. • To enhance personal productivity. This includes using word processing, spreadsheet, calendar and time reporting facilities.

DON'T	**Employees must not use the dealership's computer and Internet access facilities for activities that are not related to their jobs and professional skills improvement, or to the dealership's business. The following are some examples of inappropriate use of the dealership's facilities** • Don't use the dealership's computer and network facilities to engage in any illegal and/or unauthorised activities or to access or transmit any offensive material that may damage, compromise or jeopardise the dealership's or TMCA's legal position and reputation. • Don't distribute dealership and TMCA information assets, including financial, tech tips, business and other confidential information, outside of the dealership. This can compromise the dealership's competitive position and would be a breach of your legal obligations. • Don't share your user ID with another party. Your user ID entitles you to certain privileged information that the other party may not be authorised to access. Keep your user ID and password confidential. • Don't use the dealership's facilities for general and non-business related Web surfing. This includes playing computer games, visiting investment, stock brokerage, e-shopping and pornography websites, or downloading music and video files. Not only would such activity impact your personal productivity and distract your focus from your job, you may also contract computer viruses that are harmful to the dealership's IT environment. • Don't use the dealership's facilities for personal e-mail (e.g. Hotmail, Yahoo, etc.). Opening and/or saving attachments uses up resources on the dealership's computers and can introduce computer viruses into the dealer network. • Don't install any software on the dealership's computers other than those authorised by the dealership. Unauthorised software can create a licensing exposure and uses up valuable computer resources (e.g. hard drive space and processing cycles). Spyware can be hidden in freeware downloaded from the Internet and compromise the security of the dealership's information assets. • Don't install modems on any computers, other than those designed and managed as backup to the ISP connection, or for remote support and administration of servers. Such connections can compromise the security of the dealership's networking environment. • Don't install wireless LAN (WLAN) access points without management approval and authorisation because they will open a backdoor to bypass the dealership's security management system. • Don't open or save any e-mail attachments, or files passed to you on diskettes and CDs, without first using the Anti-virus Program to scan for viruses.

Table 3 - Sample Computer & Internet Use Policy

5 Contact List

Please note – areas displayed as blank in the tables below are for you to fill with the relevant supplier details

5.1 TMCA Contacts

Support Service	Phone	Email Address	Fax
tSupport for Toyota IT systems	1800 251175	tSupport@toyota.com.au	02 97103348

Table 4 - TMCA Support Contact List

5.2 DMS Vendor (to be filled in by Dealer)

Support Service	Contact Name	Email Address	Telephone Number

Table 5 - DMS Vendor Contact List

5.3 Other Applications (to be filled in by Dealer)

For applications not provided by TMCA or your DMS vendor.

Support Service	Contact Name	Email Address	Telephone Number

Table 6 – Other Applications Contact List

5.4 Technology Partner (to be filled in by Dealer)

Support Service	Contact Name	Email Address	Telephone Number

Table 7 – Technology Partner Contact List

5.5 TMCA IT Support Process

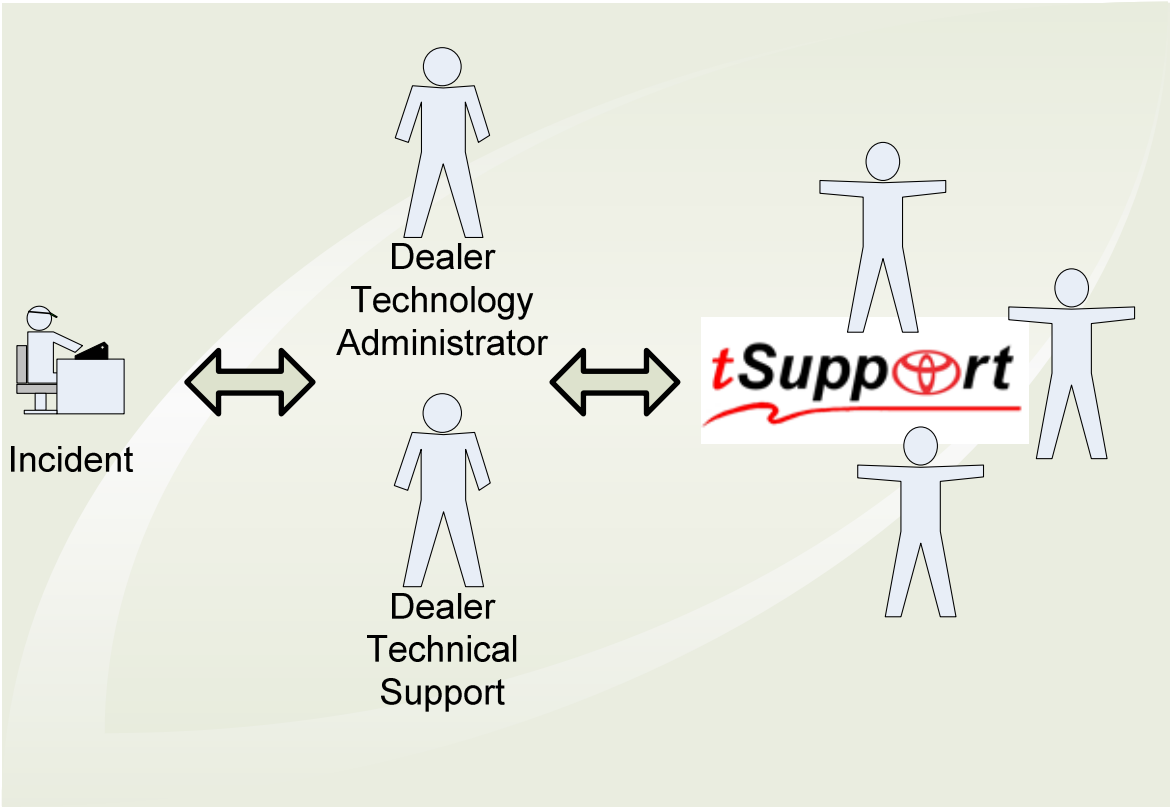

Figure 4 - TMCA IT Support Process

When a problem is encountered with your IT environment, the first step is to contact your local IT support. This is either the Dealer Technology Administrator or the Dealer Technical Support for the dealership.

If the local IT support person(s) cannot resolve the issue, then they should call tSupport on 1800 251 175 or email tSupport@toyota.com.au.

6 Technology Partner Selection Guide

This Selection Guide lists some questions and considerations to help you qualify and select the right technology partner for your dealership. Some dealers may have established internal IT departments and therefore will probably not require an external technology partner. The guide is intended for dealers needing to select a new technology partner or evaluate an existing one. It is presented in a format to allow you to score each criterion during the selection process.

	Qualification and Evaluation Considerations	Score
1	Does the vendor have the technical support skills as defined in the Staff Skills List (Table 9)? What are the vendor's core competencies?	
2	Can you define your technology support requirements? Is the vendor able to satisfy the scope of your technology support requirements? E.g. Workstation installation and maintenance, systems image and application support and maintenance, LAN and ISP connection support and maintenance, firewall/gateway and security policy installation, support and maintenance, computer emergency support, etc.	
3	Does the vendor's service level objective meet your support requirements, during and after business hours? E.g. Would the vendor be able to respond within the same business day? Can the vendor describe how it would help you resolve different situations? E.g. Restore your system images and data files, when your systems are under extensive virus attack? Can the vendor substantiate its ability to meet service level objectives?	
4	Are the vendor's support methodology and processes adequate for your environment? E.g. if the vendor provides telephone support most of the time, and charges on-site support only when required and on a time and materials basis, do you have the skills in your dealership to carry out the vendor's diagnosis instructions and install the recommended fixes?	
5	Can the vendor provide references for similar services being rendered elsewhere?	
6	Are the vendor's service charges affordable? What advantages does this vendor offer?	
7	Does the vendor have the bench strength (breadth and depth) to provide the support coverage required?	
8	Can the vendor articulate or substantiate its skills and experience claims? E.g. certifications achieved, years of experience, where and when.	
9	What is the vendor's business model? E.g. does it subcontract out work? What happens if it has more business than it can handle? Is the vendor likely to be in business next year or there after? What is its commitment to your business?	
10	What is the service termination process? Can you terminate the vendor's services easily if you are dissatisfied?	
11	Is the vendor willing to learn applications (at least the platform requirements) to support your business operations?	
12	Can the vendor demonstrate or articulate its ability to act innovatively or proactively? E.g. Will it be prepared to educate your staff to avoid recurring problems? Can the vendor help you identify better ways of managing your IT environment? Perform an update on all your workstations proactively to install a critical systems patch?	
13	Are the vendor's proposed terms of the agreement consistent with all verbal agreements? Are key terms and conditions, including rights of termination, service levels, warranties and indemnities, satisfactorily covered by the agreement?	

Table 8 - Technology Partner Selection Guide

7 Role of the Dealer Technology Administrator

The role of Dealer Technology Administrator (DTA) is critical to ensuring the smooth delivery of technology to all dealership operations. No longer are 'systems' a disconnected entity; technology is pervasive and essential to your dealership. The Staff Skills List below itemises the skills required to effectively support the dealership's IT environment. The chart includes the role of Technical Support – a role that could be filled by the Dealer Technology Administrator, another dealership employee or a third party Technology Partner. Whether the DTA fulfils the technical support role is dependent on his/her skill-set and overall job responsibilities. In most cases, outsourcing technical support is the most cost-effective strategy.

	Area of Responsibility	Systems Administrator	Technical Support	End-User
Systems	Windows	3	5	2
	Web Browser	2	5	2
	Adobe Acrobat	2	4	2
Network	Local Area Network	3	5	
	Internet Connection	3	5	
	Firewall/Gateway	2	5	
	Anti-Virus	3	5	2
MS Applications	MS Word	3	5	2
	MS Excel	3	5	2
TMCA Applications		3	4	2
DMS		3	4	2

Table 9 - Staff Skills List

1= Understand but need help to configure or use

2= Understand and can configure or use

3= Able to help others configure or use

4= Can define problem and work with tech partner or TMCA to resolve

5= Can trouble shoot and resolve most problems

Each skill level (2 to 5) requires the DTA to be able to perform specific tasks, defined as follows:

Area of Responsibility	Skill Level	Know how to…
Windows	3	1. Launch, Maximise, Minimise, Resize and Close Applications 2. Create Folders and Move Files in Windows Explorer 3. Add Local or Network Printers 4. Add/Remove Programs from Start-up Menu 5. Change Display Properties 6. Add/Remove Programs from Control Panel 7. View/Modify TCP/IP Network Properties 8. Run/Schedule Virus Scanning Software 9. Identify Application Version 10. Identify Windows Version 11. Escalate support issues (see Section 6)
Web Browser	2	1. Download Internet Explorer from Internet 2. Load the same type and version of browser on all dealership PCs 3. Add URLs to Favourites/Bookmarks 4. Enter URLs into Location/Address Bar 5. Set Default Home Page 6. Clear Cache Memory 7. Enable Content Filtering/Access Control Options 8. Escalate support issues (see Section 6)
Web-browser related software components (e.g. Adobe Acrobat Reader, Macromedia Flash, Java, etc.)	2	1. Download / upgrade required components from Infostream or the Internet 2. Know how to use the required components (e.g. using Acrobat Reader to view and print documents, using Flash to play graphics and animation, etc.) 3. Escalate support issues (see Section 6)
Local Area Network	3	1. Maintain an up-to-date Network Diagram - this means working with your network provider to ensure the diagram is current with any additions (e.g., new PCs, printers, etc) 2. Maintain records of all IT assets – including serial numbers, assigned users, hardware/software configurations, dates of acquisition, software license agreements, lease agreements, maintenance records, etc) 3. Escalate support issues (see Section 6)
Internet Connection	3	1. Measure/analyse bandwidth performance using tools like www.dslreports.com 2. Restrict/grant access to Internet for individual PCs using 'Policy Agent' software 3. Escalate support issues (see Section 6) 4. Implement backup ISP service if primary service goes down (including regular "fire drills") 5. Complete/maintain Internet connectivity Checklist (see Section 8)

Area of Responsibility	Skill Level	Know how to…
Firewall/Gateway	2	1. Grant/deny permission to sites 2. Override FW security controls 3. Enable/disable web filters 4. Report unauthorised site usage (internal/external) 5. Escalate support issues (see Section 6) 6. Complete/maintain Internet connectivity Checklist (see Section 8)
Anti-Virus	3	1. Install same type/version of anti-virus software on all PCs 2. Schedule regular updates 3. Ensure necessary fixes are implemented immediately
MS Word	3	1. Download viewer from the Microsoft website (not a full version of Word) that allows for viewing and printing of documents 2. (Alternatively) Install and launch full version of Word software 3. Demonstrate basic functionality and some more advanced functionality (e.g., mail merge) 4. Escalate support issues (see Section 6)
MS Excel	3	1. Download viewer from the Microsoft website (not a full version of Excel) that allows for viewing and printing of spreadsheets 2. (Alternatively) Install and launch full version of Excel software 3. Demonstrate basic functionality 4. Escalate support issues (see Section 6)
Delegated Administration	5	1. Launch the enrolment application 2. Create, edit and delete user profiles/ids 3. Maintain application access/entitlements for users:
Monitor Licence Agreements	4	1. Monitor compliance with vendor licence agreements (e.g. limitations on the number of PCs a program can be used on or how many personnel can access the program).

Table 10 - Dealer Technology Administrator Task List

The Dealer Technology Administrator's responsibilities include acting as the primary contact on dealership technology support-related issues. The DTA should act as liaison between the dealership and the following services:

- Technology partner;
- Call centre support (e.g., DMS Technical Assistance Centre and TMCA's Dealer Technology Support Centre (tSupport)

To fulfil all the above obligations, dealer management needs to ensure that the Dealer Technology Administrator is adequately trained at all times. This will require an ongoing commitment to education that goes beyond conventional on-the-job training. Formal training can include the services provided by the technology partner and/or courses from the various community colleges and continuing education programs.

- Upgrade or apply critical upgrades to Web browsers (i.e. Internet Explorer) and related components (e.g. Acrobat Reader, Flash, Java plug-in, etc.) upon recommendations from TMCA or your technology partner. Our direction with the web browser and related components is to recommend an upgrade once it has been proven (either through testing or application modifications) that the new browser and related component releases can work with all TMCA and business partner supplied applications.

8 Glossary

YOU CAN ALSO GO TO WWW.WHATIS.COM FOR DEFINITIONS OF THE LATEST IT-RELATED TERMS!

Term	Explanation
10BaseT	A standard for ***Ethernet*** over twisted pair cable which runs at 10 ***Mbps***.
100BaseT	A standard for ***Ethernet*** over twisted pair cable which runs at 100 ***Mbps***.
2.5G	Essentially, 2G (Second-Generation) mobile phone technology, but with some of the benefits of ***3G***. It is capable of data rates that are faster than 2G but slower than 3G.
3G	Third-Generation technology. It is used in the context of mobile phone standards. The services associated with 3G provide the ability to transfer simultaneously both voice data (a telephone call) and non-voice data (such as downloading information, exchanging email, and instant messaging).
Acrobat Approval	Software from Adobe that enables users to save eForms to their computer for completion at their convenience. Features include spell-checking and the ability to apply 128-bit encryption or password protection before submitting.
ADSL	ADSL (Asymmetric Digital Subscriber Line) is a form of ***DSL Internet access*** where the ***downstream bandwidth*** (i.e. Internet download speed to the user) is much higher than the ***upstream bandwidth*** (i.e. upload speed from the user to the Internet).
Anti-virus Program	Software that removes and protects against computer viruses.
Authentication	The verification of the identity of a user or process.
Authorisation	The validation of a user, thereby granting access to resources based on user name and password
Bandwidth	In computer networks, bandwidth is often used as a synonym for data transfer rate – the amount of data that can be carried from one point to another in a given time period (usually a second). It is measured in ***bits*** per second (bps), usually as either ***kbps***, ***Mbps*** or ***Gbps***.kilobits per second (thousands of bits per second), megabits per second (Mbps, or millions of bits per second) and in
BDSL	Business Digital Subscriber Line, a similar technology to ADSL, but operating on a higher tolerance infrastructure.
Bit	Short for binary digit – the smallest unit of data in a computer. A bit has a single binary value, either 0 or 1.
Bluetooth	A short-range wireless specification that allows connection between devices within a 10 metre range of each other; e.g. connecting a keyboard to the PC central processing unit.
Broadband	An ***Internet*** connection with a wide ***bandwidth*** allowing for more information to be transmitted in a given amount of time than is possible with ***dialup Internet access***. In Australia, an Internet connection is generally considered to be broadband if it is greater than 200 kbps.
Browser	A computer program that facilitates connection to World Wide Web (WWW) sites and allows viewing hypertext documents and “web pages”. Common Browser programs are *Mozilla Firefox, Apple Safari, Google Chrome,* and *Microsoft Internet Explorer*.

Term	Explanation
Bus	A path along which electronic signals are transmitted and received by any device attached to the signal line – that is, the way one part of a computer communicates with another. USB, which stands for Universal Serial Bus, is one example.
CDR	Consignment Discrepancy Report
Cable Modem	A device provided by Cable companies to facilitate ***broadband*** Internet access.
CDROM Drive	Compact Disk Read Only Memory Drive – A device that enables computers to read information recorded on a compact disk (CD).
Cellular	A general name for analog and digital networks that divide large areas into smaller areas called cells. As a user moves from cell to cell, his/her connection is handed off without interruption.
COSI	This refers to a retail sales order in SAP (Customer Order Sales Information)
Cookie	Some websites place a "cookie" on your computer when you visit them so that they can see what you did on your last visit and add more information if you return to the sites.
COWT	Customer Order Web Tacking
DANV	Dealer Area Network Vehicles – the dealer front end access to SAP
Dialup Internet Access	Analog Internet access available over regular telephone copper wire with a maximum ***bandwidth*** of 56 kbps.
DBMS	Data base management system
DBMS	Dealer business management system
DMS (aka DBS)	Dealer Management System or Dealer Business System.
DNS	Domain Name System, a service that translates domain names into ***IP*** addresses. Because domain names are alphabetic, they're easier to remember. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address.
Downstream Bandwidth	In telecommunications generally, a transmission from an information ***server*** toward an end user is referred to as "downstream", while transmissions from user to the server is referred to as "upstream".
DOSI	Dealer Order Sales Information
DRIP	Dealer Regional Intranet Portal – AKA Regions
DSL Internet Access	DSL (Digital Subscriber Line) is a technology for bringing high-bandwidth information to homes and small businesses over ordinary copper telephone lines. xDSL refers to different variations of DSL, such as ADSL and SDSL. Assuming your home or small business is close enough to a telephone company central office that offers DSL service, you may be able to receive data at rates up to 6.1 megabits (millions of bits) per second (of a theoretical 8.448 megabits per second), enabling continuous transmission of motion video, audio, and even 3-D effects. More typically, individual connections will provide from 1.544 Mbps to 512 kbps downstream and about 128 kbps upstream. A DSL line can carry both data and voice signals and the data part of the line is continuously connected. DSL installations began in 1998 and will continue at a greatly increased pace through the next decade.

Term	Explanation
DSLAM	A Digital Subscriber Line Access Multiplexer (DSLAM) is a network device, usually at a telephone company central office, that receives signals from multiple customer Digital Subscriber Line connections and puts the signals on a high-speed backbone line using multiplexing techniques.
DSR	Dealer Sales Reporting
Dual Band Mobile Phone	A mobile phone that can pick up analog signals when a digital signal fades. The handset operates on both 900 MHz cellular and 1800 MHz PCS frequencies.
DVD ROM Drive	A device that enables a PC to read information recorded on a DVD (Digital Video Disk) or CD (Compact Disk).
Dynamic IP Address (DHCP)	Many ***Internet Service Providers*** limit the number of ***Static IP Addresses*** they allocate, and economise on the remaining IP addresses they possess by temporarily assigning an IP address to a requesting computer from a pool of IP addresses. The temporary IP address is called a dynamic IP address. Assigning dynamic IP addresses requires DHCP (Dynamic Host Configuration Protocol).
e-Business	e-business (electronic business), derived from such terms as “e-mail” and “e-commerce,” is the conduct of business on the ***Internet***, not only buying and selling but also servicing customers and collaborating with business partners to drive efficiencies, speed, innovation and new value creation in and across organisations.
e-Commerce	A particular e-business initiative that focuses on individual business transactions, using the ***Internet*** as a medium of exchange, including B2B and B2C.
e-Marketplace	Electronic forum where business communities team with one another to leverage/streamline commerce and transactions.
Encryption	An algorithm applied to data, usually during transmission, to make it unreadable by those who are unauthorised. Decryption is the reverse process to convert the data back to a readable format.
Ethernet	The name given to a large and diverse family of computer networking technologies that operates at many speeds for ***local area networks***. Ethernet uses twisted-pair or coaxial cable and runs usually at speeds of 10 Mbps or 100 Mbps.
Exchange	A virtual marketplace that brings multiple buyers and sellers together and enables them to transact at a dynamic price, governed by the rules of the exchange.
Firewall	An enterprise with a local area network (***LAN***) that allows its workers access to the wider ***Internet*** will often install a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to. A firewall is often installed in a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources.
(Adobe) Flash	Flash is a software package, distributed by Adobe, specifically designed for the creation of online animated presentations (including video, sound, text and graphics). Flash files are identified by .swf and .flv (Flash Video) extensions. The Flash Player program, downloadable free from the Adobe website, is required to display Flash contents created using the Adobe Flash Professional program.

Term	Explanation
Gateway	A gateway is a network point that acts as an entrance to another network. On the ***Internet***, a node or stopping point can be either a gateway node or a host (end-point) node. Both the computers of Internet users and the computers that serve pages to users are host nodes.
Gbps	Gigabits per second, or billions of ***bits*** per second. Used to measure ***bandwidth***.
GHz	GigaHertz – 1,000 Mhz or 1,000 million cycles per second – a measurement commonly used to indicate processing speed or capacity.
GIF	GIF (Graphics Interchange Format) – originally created by CompuServe, it is now the most common format for compressed graphics on the ***Internet***.
GPRS	General Packet Radio Service – a 2.5 G packet-based "always on" technology implemented in GSM networks enabling wireless data transmission speed of up to 114 Kbps.
GSM	Global System for Mobile Communications – a widely 2G wireless digital cellular/PCS standard.
HTML	HTML (HyperText Mark-up Language) – the set of mark-up symbols or codes inserted in a file intended for display on a Web browser. The mark up tells the **Web browser** how to display the information for the user.
Hub	A hardware device used to interconnect circuits together to form a local area network (***LAN***). An Ethernet Hub is one that supports the IEEE 802.5 protocol
Internet	The ubiquitous global network linking millions of computers together to form the information highway.
Internet Service Provider	Internet Service Provider is a company that provides individuals and companies access to the Internet and other related services such as website building and virtual hosting. An ISP has the equipment and the telecommunication line access required to have POP (point-of-presence) on the Internet for the geographic area served. The larger ISPs have their own high-speed leased lines so that are less dependent on the telecommunication providers and can provide better service to their customers.
Intranet	A network, internal to an organisation, that uses ***Internet*** technologies and functions to provide services to its users. It usually has no public access.
IP	Internet Protocol – the method or protocol by which data is sent from one computer to another on the ***Internet***. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.
IP Address	Internet Protocol address – used by computers to locate and talk to each other on the Internet, much the same way people use phone numbers to locate and talk to one another on the telephone.
ISDN Internet Access	Integrated Services Digital Network (ISDN) is a form of digital transmission over ordinary telephone copper wire as well as over other media. Home and business users who install an ISDN adapter (in place of a modem) can see highly-graphic Web pages arriving very quickly (up to 128 Kbps).
ISP	*See **Internet Service Provider***
ISP Connection	Same as "Internet Connection".
IT	Information Technology.

Term	Explanation
Java	A cross-platform programming language used extensively on the Net. Using a Virtual Machine concept, a Java program can works on all computer platforms. Java can be used to create entire applications or to build small application modules or applets for use as part of a Web page. Applets make it possible for a Web page user to interact with the page.
Java Plug-in	Java Plug-in technology, included as part of the Java 2 Runtime Environment, Standard Edition (JRE), establishes a connection between popular browsers (e.g. Internet Explorer) and the Java platform. This connection enables applets on websites to be run within a browser on the desktop.
JPEG	A file format for compressing and displaying images (e.g. photographs) on the Web.
Kbps	Kilobits per second, or thousands of **bits** per second. Used to measure **bandwidth**.
LAN	A local area network (LAN) is a group of computers and associated devices (e.g. printers) that share a common communications line and typically share the resources of a single processor or ***server*** within a small geographic area (for example, within an office building). Usually, the server has applications and data storage that are shared in common by multiple computer users.
MAC Filtering	Devices connect to ***LAN***s using network cards. Each network card has its own unique MAC (Media Access Control) address. 'MAC Filtering' is a network security measure that allows only devices containing network cards with specific MAC addresses to access the network.
Mbps	Megabits per second, or millions of ***bits*** per second. Used to measure ***bandwidth***.
MHz	Mega Hertz or 1 million cycles per second – a measurement commonly used to indicate processing speed or capacity.
MPEG	The standard for compressing audio and video files to send over the ***Internet***.
MSJVM (Microsoft Java Virtual Machine)	MSJVM is a technology that was included in some versions of Microsoft Internet Explorer, a component of Microsoft Windows®. This technology allows certain types of programs, called Java applications or Java applets, to run on Windows-based computers. In the April 2004 settlement with Sun Microsystems, Microsoft is no longer allowed to distribute MSJVM nor enhance current codes. Microsoft will continue to address security issues and provide guidance to help customers migrate from MSJVM until December 31, 2007. Windows customers with applications that rely on MSJVM must seek an alternate solution before then.
Modem	Modulator-demodulator – a device that converts a digital signal to analog and vice versa, allowing computer data to be transmitted over voice lines.
Multimedia	Multimedia is the simultaneous use of multiple presentation mediums to communicate. The term often is used to denote the use of sound along with animation, text, and/or video.
Network Address Translation	Network Address Translation (NAT) is the translation of an ***IP*** address used within one network to a different IP address known within another network. A typical scenario in multi-franchise Dealerships.
NIC	Network Interface Card – a printed circuit board that allows a computer to connect to a network.

Term	Explanation
NTU	Network Termination Unit – a device that connects the PSTN with a CPE. This device marks the final interconnect between the public network and a customer's private equipment. The NTU is owned by the service provider and typically has communication standards, such as voltages and protocols, which allow specific types of equipment to communicate with the PSTN.
OEM	Original Equipment Manufacturer – mainly used in this document to refer to an Auto Manufacturer.
Packet	When a file (e.g. email message, HTML file etc) is transmitted over the ***Internet***, ***WAN*** or ***LAN***, the TCP layer of ***TCP/IP*** divides the file into "chunks" – called "packets" – which are small enough for efficient transmission. Once all the packets have arrived, they are then reassembled into the original file (by the TCP layer on the receiving end).
Packet Shaper	A hardware device and application that monitors, controls, and accelerates data packets performance over the WAN. Essentially, a data traffic controller.
PC Client	A Personal Computer or PC workstation.
PCS	Personal Communication Services – a general name used to refer to 2-way digital networks with integrated voice, data and messaging capabilities.
PDA	Personal Digital Assistant – a small hand-held computing device, usually based on the Microsoft Pocket PC standard or Palm OS.
PDF	Portable Document Format – a file format created by Adobe, initially to provide a standard form for storing and editing printed publishable documents. Documents in PDF format are very common because they can be easily seen and printed by users on a variety of computer and platform types. The Adobe Acrobat Reader, available free from Adobe, is required to read PDFs.
Plug and Play (PnP)	A device or card that can be connected/inserted into the computer and be automatically recognised and configured to work in the system. PnP has greatly simplified the process of upgrading computers by enabling users to add new devices or replace existing ones. PnP was made possible since the introduction of Windows 95.
Plug-in	Plug-ins are programs that work with a ***browser*** to read and display a certain type of file. They are relatively small pieces of software, so it doesn't take users forever to download them off the ***Internet***. They are specifically designed to work with a particular type of file (e.g. audio or video file), so they can accomplish a lot of things that a basic browser can't.
Portal	Typical services offered by portal sites include a directory of websites, a facility to search for other sites, news, weather information, e-mail, stock quotes, phone and map information, and sometimes a community forum. Excite is among the first portals to offer users the ability to create a site that is personalised for individual interests.
Protocol	A set of rules governing the communications between network devices.
PPP	PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a ***server***. For example, your ***Internet Service Provider*** may provide you with a PPP connection so that their server can respond to your requests, pass them on to the ***Internet***, and forward your requested Internet responses back to you.

Term	Explanation
Proxy Server	In an enterprise that uses the ***Internet***, a proxy server is a ***server*** that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server is associated with or part of a gateway server that separates the enterprise network from the outside network and a ***firewall*** server that protects the enterprise network from outside intrusion.
Quality of Service	Performance measurement of a transmission service; usually expressed in terms of network throughput or response time and availability.
QuickTime	A file format, developed by Apple Computer Inc., commonly used for the delivery of video, animation, and sound through a webpage or website, as an alternative to MPEG or Flash. Viewing QuickTime files on the web requires the download and installation of the QuickTime player or plug-in from the Apple Computer website. The MOV movie file format is used by QuickTime. However, QuickTime also supports most encoding formats, including Cinepak, JPEG, and MPEG.
RAM	Random Access Memory – the place in a computer where the operating system, application programs and data used at the time are kept so that they can be quickly reached by the computer's processor. RAM is much faster to read from and write to than the other kinds of storage in a computer, the hard disk, floppy disk, and CD-ROM. However, the data in RAM stays there only as long as your computer is running. When you turn the computer off, RAM loses its data. When you turn your computer on again, your operating system and other files are once again loaded into RAM, usually from your hard disk.
RealPlayer	A plug-in application developed by Real Networks that allows a user to hear audio and video saved in various file formats. Realplayer also plays streaming media, that is, audio or video that is broadcast live over the ***Internet***. Clicking on some hyperlinks will cause your browser to activate RealPlayer.
Router	A device acting as a traffic cop to direct data packets to the proper destination.
Search Engine	A database of information on URLs linked to certain keywords. ***Internet*** users can use this data to find the information they need (e.g. Google).
Smartphone	A combination of a mobile phone and a PDA.
Scalability	Scalability is the ability of a computer application or product (hardware or software) to continue to function as it (or its context) changes in size or volume in order to meet changing user needs. Typically, the rescaling is to a larger size or volume.
SDSL	SDSL, or symmetric DSL, offers the same ***upstream*** and ***downstream bandwidths***. *See **DSL Internet Access** for a detailed description of DSL.*
Server	In general, a server is a computer program that provides services to other computer programs in the same or other computers.
Service Level Agreement	An agreement between customer and service provider guaranteeing a certain quality of service,
SSL	SSL (Secure Socket Layer) is an encryption system built into Web ***servers*** and ***browsers*** that uses "certificates" of identity to authenticate websites and surfers. These certificates are digitally signed and issued by a trusted third-party such as VeriSign.
Stacked Modems	Two or more analog modems that are banded together to achieve a higher overall ***bandwidth***. For example, stacking three 56 kbps modems theoretically produces an aggregate bandwidth of 168 kbps.

Term	Explanation
Static IP Address	A Static IP address is where a computer uses a permanent ***IP address*** every time it logs on to a network, for example the ***Internet***.
TCP/IP	Transmission Control Protocol / Internet Protocol – a set of de facto standards developed / endorsed by the IETF (Internet Engineering Task Force) to facilitate communications between communication devices and networks.
Thin Client	A low-cost computer devoid of a CD-ROM player, diskette drive and expansion slots. Thin clients are designed to operate on a network and run applications where the majority of the processing is handled by the central ***server***. They are generally used for browsing the ***Internet*** or remote desktop software. Some of the advantages of thin clients include: lower hardware costs, easier security and the ability to manage a group of computers centrally.
Tri-Band	Triband phones (also known as tri-band or tri-mode) are mobile phones that support the GSM 900/1800/1900 MHz bands.
TSO	Technical Services Operations
TVOPS	Toyota Vehicle Ordering Processing System
Upstream Bandwidth	*See **Downstream Bandwidth***
UNIX	A computer operating system developed by Bell Laboratories. UNIX is used widely as the operating system for web ***servers***. Different vendors may use a different name to refer to their implementation of UNIX.
UPS	Uninterruptible Power Supply – a device that stores electricity to supply power to other devices in the event of power failure.
USB	Universal Serial Bus – an external computer connection that offers speeds up to 12Mbps/1.5MBps (USB 1.0/1.1) and 480Mbps/60MB per second (USB 2.0). Originally designed for keyboards and mice, it's now commonly used to connect a PC to an external device, such as a flash memory drive or a CD burner.
URL	Universal Resource Locator – text name to facilitate connection to ***Internet*** websites (e.g. www.toyota.com.au).
UTP	Unshielded Twisted Pair is the most common kind of copper telephone wiring. Twisted pair is the ordinary copper wire that connects home and many business computers to the telephone company. To reduce crosstalk or electromagnetic induction between pairs of wires, two insulated copper wires are twisted around each other. Each signal on twisted pair requires both wires. Since some telephone sets or desktop locations require multiple connections, twisted pair is sometimes installed in two or more pairs, all within a single cable. For some business locations, twisted pair is enclosed in a shield that functions as a ground. This is known as shielded twisted pair (STP).
WAN	Wide Area Network – communications facilities enabling computers and terminals (stand-alone or connected to local area networks) to communicate over long distance.
Web Browser	*See **Browser***
Web Master	A person in charge of a Website.
Web Messaging	An interface runs on any industry-standard ***Web browser*** on a multimedia computer connected to the ***Internet*** or an ***intranet***. Web messages are used to update dealer's vehicle stock inventory or invoicing to Dealer Management System via tJunction

Term	Explanation
WEP	Wireless Equivalent Privacy – a security feature using a key installed in wireless ***LAN*** stations and access points to encrypt/decrypt transmission.
Windows Media Player	A software program included in the Microsoft OS, or that can be downloaded for free from Microsoft, to play back contents created by Microsoft Windows Media programs (e.g. Windows Media 9 Series), usually with .wma or .wmv file extension, or common mp3, jpeg or mpeg files.
Wireless	The term wireless refers to telecommunication in which electromagnetic waves (rather than some form of wire) carry the signal over part or all of the communication path.
Wi-Fi	Wireless Fidelity, usually used to refer to Wireless Ethernet
XGA	**XGA** (*extended **g**raphics **a**rray)* is a high-resolution graphics standard capable of displaying 640 by 480 or 1024 by 768 resolutions. **SXGA** (***S**uper **Ex**tended **G**raphics **A**rray)* is capable of displaying 1280 x 1024 resolution, or approximately 1.3 million pixels. ***UXGA (U**ltra **Ex**tended **G**raphics **A**rray)* is capable of displaying 1600 x 1200 resolution, or approximately 1.9 million pixels. **WSXGA** (**W**ide SXGA) is capable of displaying 1600 by 900 and 1600 by 1024 resolutions.
XML	Extensible Markup Language – a technology for creating web content. It can operate over multiple devices and network platforms.

Appendix A

The following table represents informal testing carried out by TMCA as to application functionality when later versions of Internet Explorer (other than V6.0) are used to run TMCA applications.

This table is to be used as a guide only, and until TMCA can carry out formal studies and publish results, it can not assume any responsibility, nor will it be able to provide support, if a dealership decides to install later version of Internet Explorer in their local environment and experiences issues.

Legend:

TBA =	To be advised
D =	May work, but there are dependencies on additional upgrades
N =	Will not work
P =	Potentially should work

+Name	Description	Vista	Windows 7	IE7.0	IE8.0	Dependancies
AFI	Accessory Fitment Instructions	TBA	TBA	P	P	
Body & Paint	Registration for Smash repairers	TBA	TBA	P	P	
Careers	GTR Support and Recruitment tools	TBA	TBA	P	P	
CDR	Consignment Discrepancy Report	TBA	TBA	P	P	
COWT	Track my New Toyota	TBA	TBA	P	P	
Customer Experience Reporting	CSI website	TBA	TBA	P	P	
Dealer Scorecard	Reporting tools for sales and CSI	TBA	TBA	P	P	
Delegated Admin	LDAP Admin tool	TBA	TBA	P	P	
DSR	Daily Sales Report	TBA	TBA	P	P	
Elasticity Rebate	Rebates for parts sold at less than retail	TBA	TBA	P	P	
Fleet	myFleet Application	TBA	TBA	P	P	
iCrop	Service Scheduling	TBA	TBA	P	P	
Parts-Core	Mainframe parts system	D	D	TBA	TBA	3270 Emulator - Upgrade needed - recommend Mocha 3270
Parts-Stock Locator	Finding stock at other dealers	TBA	TBA	P	P	
Parts-TDOS	Parts Stock Orders, Heijunka and invoices	TBA	TBA	P	P	
PPS	Pre Paid Service	D	D	TBA	TBA	3270 Emulator - Upgrade needed - recommend Mocha 3270
Professor	A tool that demos and teaches about the features of new cars	N	N	TBA	TBA	Sun JRE 1.6+
Regions-DRIP	Dealer Regional Intranet Portal	TBA	TBA	TBA	TBA	
SAP - DANV	Vehicles	D	TBA	TBA	TBA	SAP GUI - upgrade needed to 7.1
SAP - Warranty	Winpaq Support	D	TBA	TBA	TBA	SAP GUI - upgrade needed to 7.1
SARIS	Service Manuals	TBA	TBA	P	P	
Showroom Direct	Sales tool	P	P	TBA	TBA	Sun JRE 1.6+
TIPS	Toyota Integrated Planning System	TBA	TBA	P	P	
tMail	Dealer Email list generater & replication	TBA	TBA	P	P	
TVOPS	Order Planning	TBA	TBA	P	P	

Appendix B

TOYOTA

I.T. Checklist

This *I.T. Checklist* is your quick reference for the key hardware and software requirements for your dealership. It allows you to assess your I.T. readiness to leverage both TMCA and non-TMCA I.T. business applications to facilitate operational excellence at your dealership.

The parameters apply to all dealer categories.

DESKTOPS

Desktops should be less than 3 or 4 years old, running Windows XP with the latest security patches and anti-virus software. You should only purchase new equipment that meets or exceeds the recommended levels. This will ensure that the new workstations will have a useful life span of at least 4 years.

Processor

- ☐ Current processor (such as the current Intel family).
  Minimum: 1.66GHz
  Recommended: 2.4GHz or higher, dual core

Memory

- ☐ Minimum: 1GB RAM
  Recommended: 2GB or higher

Disk

- ☐ Minimum: 20GB Hard Drive
  Recommended: 100GB Hard Drive

Network Card

- ☐ Standard 100Mbps Network Interface Card (Wired)

Display

- ☐ Resolution: 1024 x 768 minimum

Optical Drive

- ☐ DVD ROM

Other

- ☐ Audio Card
- ☐ At least 2 USB 2.0 ports

Operating System

- ☐ Microsoft Windows XP Professional – SP3, 32-bit
- ☐ Administrative access to the Operating System during software installation

Applications

- ☐ Microsoft Internet Explorer v6.0*
- ☐ Windows Media Player v6.0 or later
- ☐ Adobe Flash for Internet Explorer v6.0
- ☐ Latest version of Acrobat Reader
- ☐ Latest version of Quicktime
- ☐ Version 1.6 of Sun JRE or later
- ☐ Symantec or McAfee Antivirus – with current subscription for regular updates
- ☐ MS Office 2003 or MS Office Viewer depending on job function
- ☐ Essential software installed only

Please refer to sections 2.3.1 and 2.3.2 of the Dealership IT Guide for more information.

* Note: Windows Vista and Internet Explorer 7+ have known issues with TMCA software and are not recommended for use. TMCA are formally reviewing functionality of applications with later versions of Internet Explorer and will update this checklist accordingly.

SERVERS AND PRINTERS

Local Servers

- ☐ Current servers running recent version of server software with patches installed.

  Please refer to section 2.6.2.3 of the Dealership IT Guide for more information.

Printer

- ☐ Shared printer(s) available on the network.

  Please refer to section 2.3.4 of the Dealership IT Guide for more information.

TOYOTA

I.T. Checklist

NETWORK

The network should be a wired network, professionally installed and configured with necessary routing rules.

Network Switch

☐ 100 Mbps or higher.

Please refer to section 2.4.2 of the Dealership IT Guide for more information.

Cabling

☐ Category 5 or higher.

Please refer to section 2.4.3 of the Dealership IT Guide for more information.

DAN

☐ Must have a DAN (Dealer Access Network) connection which will enable access to TMCA applications.

Please refer to section 2.4.5 of the Dealership IT Guide for more information.

Security

☐ Firewall or similar appliance professionally configured.

Please refer to section 2.4.7 of the Dealership IT Guide for more information.

Wireless

☐ WLAN solution professionally configured.

Please refer to section 2.4.4 of the Dealership IT Guide for more information.

Routing

☐ The DAN router must have routes to the following networks pointing towards the NEC DAN router:

- 192.168.108.0 /24
- 192.168.109.0 /24
- 10.9.100.0 /24
- 10.12.100.0 /24

Please refer to section 2.4.6 of the Dealership IT Guide for more information.

DNS

☐ Forwarding configured for zones of tmca.com.au and toyota.com.au as outlined;

- Primary DNS – 192.168.109.38
- Secondary DNS – 192.168.109.138

Please refer to section 2.4.11 of the Dealership IT Guide for more information.

Network Diagram

☐ Maintain an up-to-date Network Diagram.

Please refer to section 2.4.12 of the Dealership IT Guide for more information.

SECURITY

Avoid common security risks to protect your network and computers from malicious users and the Internet.

Desktops and Servers

☐ Windows running current security patches.

Please refer to section 2.6.2.3 of the Dealership IT Guide for more information.

☐ Anti-virus installed and up-to-date.

Please refer to section 2.6.2.1 of the Dealership IT Guide for more information.

Passwords

☐ Secure storage of passwords.

Please refer to section 2.6.2.5 of the Dealership IT Guide for more information.

☐ One password per person – no sharing.

Please refer to section 2.6.2.5 of the Dealership IT Guide for more information.

☐ Password protected desktops and servers.

Please refer to section 2.6.2.5 of the Dealership IT Guide for more information.

Internet

☐ No access to desktops or servers from outside the dealership(s).

Please refer to section 2.6.2.2 of the Dealership IT Guide for more information.

TOYOTA

I.T. Checklist

GENERAL

Support

- ☐ In the absence of in-house technical resources, contract the services of a local technology partner.
  Please refer to section 2.5.1 of the Dealership IT Guide for more information.
- ☐ Screen the services of potential technology partners by using the Technology Partner Selection Guide in the Dealership IT Guide.
  Please refer to section 7 of the Dealership IT Guide for more information.
- ☐ Maintain an up-to-date contact list of IT support contacts including TMCA, DMS vendor and your technology partner.
  Please refer to section 6 of the Dealership IT Guide for more information.

Staff Skills

- ☐ Establish a computer and Internet policy to advise staff on appropriate and inappropriate use of the dealership's computer and networking facilities. Refer to a sample policy in the Dealership IT Guide.
  Please refer to section 5 of the Dealership IT Guide for more information.

Software

- ☐ Authorised software only on all desktops and servers. No games, browser extensions, peer-to-peer downward tools, or other unnecessary software installed.
  Please refer to section 2.6.1.2 of the Dealership IT Guide for more information.

ADVANCED

For higher security and performance where the organisation has professional IT support available.

Security

- ☐ Centrally-managed user accounts on Windows Domain Controller.

Network

- ☐ Internet Web Proxy server installed and configured.

Email

- ☐ One email address for each staff member.

For more information, please contact tSupport on 1800 251 175, email tsupport@toyota.com.au or visit regions.tmca.com.au and click "your region\tsupport"

POINT XXXX