Protected

Toyota Motor Sales, U.S.A., Inc.

TMS FILE TRANSMISSION SECURITY STANDARD

Protected

TMS File Transmission Security Standard

1. Purpose

The purpose of this Standard is to define requirements regarding the protection of files transmitted over public networks. This Standard supports the Confidentiality, Integrity and Availability of TMS Information and Information Assets by defining the acceptable methods of file transmission.

2. Scope

The rules and recommendations set forth in this Standard govern the actions of TMS, its Associates, Contingent Workers and Business Partners as those actions pertain to TMS Information and Information Assets. The controls and standards set forth in this Practice apply to Information and Information Assets owned by or under the control of TMS, regardless of physical location.

3. Definition

3.1. File Transmission Protocol (FTP)

3.2. **File Transfer Protocol over SSL/TLS (FTPS)** – A secure, encrypted file transfer method using standard FTP protocol over Secure Socket Layer (SSL) or Transport Layer Security (TLS).

3.3. **Pretty Good Privacy (PGP)** – A computer program used for the encryption and decryption of data

3.4. **Secure Sockets Layer (SSL)** – A method to encrypt data typically sent over the Internet. SSL is implemented in web browsers so you can visit secure websites. It can also be implemented in other connections like e-mail for corporate users.

3.5. **Secure File Transfer Protocol (SFTP)** – A fully interactive replacement for FTP is Secure File Transfer Protocol (SFTP) and is supported on most modern computer operating systems. SFTP, part of the Secure Shell (SSH) suite of utilities, offers strong authentication, and session integrity and encryption.

3.6. **Private / Trusted Network –** TMS Trusted Networks:

3.6.1. TMS Local Area Networks (LAN)

3.6.2. Point to point private networks with TMS sites and data centers

3.6.3. Encrypted links over a frame/shared network to a TMS network

3.6.4. Partner connection routed through a private link without encryption e.g Dealer Network

3.7. **Internet / Untrusted Network** – It includes

3.7.1. Partner connections routed through the Internet without encryption.

3.7.2. The Internet

4. Standard

Electronically exchanging TMS information carries with it the risk of sensitive data falling into the wrong hands, or not even making it into the right hands. File Transmission Protocol (FTP) and many other commonly used file transfer methods do not have any built-in security, exposing data to eavesdropping, illegitimate modification, and unauthorized access. This makes it essential for secure, efficient and reliable ways of file transmission.

4.1. Requirements for Secure File Transmission

4.1.1. File Transmission System Configuration

The following should be used where possible

a) Disable Anonymous Access - Users should be made to authenticate to use a file transfer service

b) Account Security

- Access to files and directories should be based on a need to know basis and follow the principal of least privilege to control access to data
- Third party service accounts should be uniquely assigned to TMS and must not be shared

c) Password Policies

Service account passwords:

- Should include at least 2 numbers, 2 uppercase characters, 2 lowercase characters, and 2 special characters or symbols
- Should be at least 16 characters in length.
- Are considered Confidential Information and should be communicated only to authorized personnel, using either encryption or an out-of-band method (e.g. telephone).
- Should not be transmitted using unencrypted protocols such as email.
  Note: Acceptably strong service account passwords can be generated here http://tv/EISP/Documents/0b37454a-2fdb-4f62-aaa4-dced2422a8cbservice_account_password.html

d) Activity Logging

- File transmission servers should log all access and administration events
- The file transfer log should be collected, analyzed, retained and reviewed

e) File transmission servers should disable directory listing.

f) TMS files should be retained on Supplier servers used for file transmission only as long as necessary for processing

4.2. File Delivery

A secure file transmission should be used to protect files transmitted over Untrusted networks.

Acceptable encryption methods include: VPN, SSL, FTPS, SFTP and PGP.

4.2.1. FTP is acceptable on trusted networks and end to end VPN connections where alternatives are not available.

4.2.2. FTP is acceptable without network-layer encryption to transmit PGP-encrypted files.

4.2.3. Encrypted files must be decrypted on non-perimeter servers only (within internal DMZs).

Network Type	Acceptable Delivery Method
Private / Trusted Network	FTP, FTPS, SFTP
Internet / Untrusted Network	FTP with VPN, FTPS, SFTP, FTP using PGP

5. Adoption

The implementation of this Standard and related Practices and Procedures is expected to be adopted over a reasonable period of time so as to not disrupt business operations.

6. Audit

Compliance with this Practice is subject to audit by Management, Internal Audit, and/or EISP.

7. Exception

There may be instances where there is a justifiable business need to perform actions that are in conflict with TMS Standard. TMS recognizes that policies, standards and practices cannot be created and enforced to address all business issues. The following principles apply to exceptions:

7.1. Exceptions should have a justifiable business case, and documented approval from the Information Owner and appropriate stakeholders.

7.2. Exceptions are valid for one year at which time the exception must be reevaluated and re-approved.

7.3. If exceptions will circumvent existing internal controls, then mitigating or compensating controls should be implemented.

8. Related Policies and Procedures

8.1. TMS Information Security & Privacy Management Policy

8.2. TMS Information Classification Practice

8.3. TMS Logging & Monitoring Practice

8.4. TMS Access & Authorization Practice

8.5. TMS Encryption Standard

9. Review

This Standard shall be reviewed every two years or as necessary from the date of approval.

Revision Record

Version/Revision	Date	Author	Description	Section(s) affected
V0.1	02-24-10	Infosys Team	Base Document	All Section