

RepliWeb-MFT & Israeli Directives 357 and 257

The Israeli Supervisor of Banks “Proper Conduct of Banking Business - Information Technology Management” Directive 357 (2003), and Supervisor of the finance sector in the MOF “Directive for Information Security Management in enterprises” no. 257 (2006) set requirements for Information Security management and mechanisms in the finance sector.

RepliWeb-MFT helps customers to meet these strict information security requirements by securing and auditing the internal and external exchange of sensitive electronic data.

Requirement	R-MFT Features
User Authentication	<ul style="list-style-type: none"> Personal user account for each user User accounts can be defined in RMFT or in Active Directory Support for group settings (R-MFT / Active Directory) User passwords are protected in storage
Access Control	<ul style="list-style-type: none"> Personal User account for each user RMFT use is permitted only to authorized users User folder access is permitted according to specific user / group permissions Support for Active Directory user management mechanisms, including groups and roles Separate roles for Administrator and Users Support for IP / Port-based access control
Encryption	<ul style="list-style-type: none"> Transferred data is encrypted using AES (256 bit), Triple DES (168 bit) or RC4 (128 bit) Data at rest is encrypted using AES (256 bit) User passwords are protected in storage (When using Active Directory, all passwords are protected by Microsoft Active Directory industry-standard mechanisms) Mandatory use of encrypted protocols
Integrity	<ul style="list-style-type: none"> Package-level and file-level integrity checks User / administrator-defined integrity checks, using inspection policies (e.g. malware checks) Integrity checks for administrative messages Comparison of source and target files Encryption of transferred data prevents interception and modification while in transit
System and Data Availability	<ul style="list-style-type: none"> Configuration and Data backup and restore mechanisms Front-end load balancing Cluster support
Audit Mechanisms	<ul style="list-style-type: none"> Login / logout activity is logged All package and file transfer activity is logged Automated (host to host) transfers are logged Interfaces with Microsoft FTP server are logged Integration with Windows Event Viewer

Key Benefits

- Secure the electronic exchange of financial data
- Meet requirements for file security and access control
- Encrypt data at-rest and in-transit

Prepared by Alfa Consulting

This analysis was prepared by Alfa Consulting. Alfa specializes in developing effective security architectures for products and services and assists vendors with regulatory compliance.

For More Information:

Americas: +1 954-946-2274

EMEA: +44 208-544-8070

email: sales@repliweb.com

URL: www.repliweb.com

RepliWeb

an  ATTUNITY company